HP Hub & Switch Management for OV-UX

User Guide

Publication Number

Edition 2
February 1999

Applicable Product

HP Hub & Switch Management for OV-UX

J3250N

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
http://www.hp.com/go/procurve

Contents

10 HP Hub & Switch Management Admin

11 Management for Non-Browserable Devices

Appendix A

Information About HP Hub & Switch Management for OV-UX

This chapter includes:

Introduction

This guide will help you use HP Hub & Switch Management for basic management of HP network devices.

We assume that you are a knowledgeable HP-UX system and network administrator, and have supervisory access to your network system and devices. For example, you should know the following:

- how to update your HP-UX system with new software
- how to kill processes
- how to write scripts
- how to modify X Window/Motif resources
- how to view, search, and edit files

You should understand the functions and correct operation of your network devices, such as hubs, bridges, routers, and switches. Your system should be set up to support the use of the HP OpenView platform and HP Hub & Switch Management. You should already have the appropriate network software running and know how to use your network utilities.

Features of HP Hub & Switch Management

This section presents some of the features that are included in this version of HP Hub & Switch Management.

HP Proactive Networking

HP Proactive Networking offers the combined benefits of outstanding products and effective, easy-to-use network management that provide you with the control, uptime and performance your network needs.

Control

- Increases visibility into the network by monitoring all segments and displaying network performance information
- Provides Anywhere Management with an easy-to-use Web browser interface
- Is compatible with other vendor's products

Uptime

- Finds and fixes common network problems, then informs the network administrator
- Provides high availability and high performance
  - Switch meshing for switching
  - Cisco Fast EtherChannel® for servers
- Standards-based products
- Lifetime warranty (for as long as you own the product) and free end-user telephone support

Performance

- Award winning products
- Large capacity "pipes" (up to 20 Gbps) between switches
- Provides high availability and high performance
  - Switch meshing for switching
  - Cisco Fast EtherChannel® for servers

- Scalable solutions from 10 Mbps to Gigabit Ethernet
- Blocks unwanted traffic with Protocol Filtering

HP Proactive Networking products save time, money and increase productivity. The agent-enabled, web-based management component of Proactive Networking is embedded in newly introduced HP managed hubs and switches. It consists of a Java-based Web agent and an embedded web server. In the past, if you wanted to see a graphical representation of your network or get device-specific information, you had to first load management software on a specific station and then be at that station to view the screens.

You can now use most Web browsers that supports Java and frames. There is no need to learn a new application. You see the same interface with the same look and feel —Java is operating-system independent. You can use a Web browser on any networked computer, day or night, to configure, control, and monitor networking devices (managed hubs and switches), and to query faults from any of these devices. You will immediately see the reduced cost of ownership, since the devices can be managed with minimal effort anytime, anywhere, and with any platform.

Using your Web browser, you can now perform network management functions for several HP devices.

Note: The device must have an IP address in order to be managed with a browser. The management station must also have an IP address.

Support for New Devices

For information on new devices supported by this version of HP Hub & Switch Management, see the Release Notes included on the product CD. (For product version number, see the product CD or the inside of the cover page of this manual.

Technical Product Support

Product support is available on the World Wide Web. The URL is:

http://www.hp.com/go/procurve

Click on **Support**. The information available at this site includes:

- HP network device MIBs
- HP network device firmware
- HP Hub & Switch Management frequently asked questions

In addition, you can call your HP Authorized Dealer or the nearest HP Sales and Support Office.

Before Installing HP Hub & Switch Management for OV-UX

This chapter includes:

It is assumed that your network devices are properly set up.

Support Information

If you have difficulty installing or using this product, call your HP Authorized Dealer or the nearest HP Sales and Support Office. You can also obtain information by accessing the HP World Wide Web pages at the following URL:

http://www.hp.com/go/procurve

Management Station Requirements

Hardware

The following table shows the recommendations for HP 9000 hardware.

HP 9000 Systems with HP-UX 10.20 or 11.00	
Models	all (except 705 with Series 700)
Memory (minimum megabytes)	64 MB*
Disk Space (minimum megabytes**)	150 MB
Monitor	Color with at least 1280 x 1024 resolution
Color planes	8
Mouse	Yes

* The larger your IP network or the more HP OpenView Windows (ovw) sessions you run, the more memory you will need. A good guideline is 10 megabytes for every additional 500 nodes, or 25 megabytes of memory for every additional ovw session that you expect to run.

**Includes HP OpenView Network Node Manager.

Software

The following table shows the software that must be installed, configured, and verified to run properly prior to installing HP Hub & Switch Management. These prerequisites assume that you are running a single HP OpenView Windows (ovw) session.

HP 9000 Systems	
OS version	**HP-UX 10.20 and 11.00**
OS configured swap space (minimum megabytes)	120 MB*
Type of window software	X Window with OSF/Motif/CDE
LAN software	LAN/Link for HP 9000 & ARPA Services/9000

* The more OpenView Windows (ovw) sessions you run, the more OS configured swap space will be necessary. A good guideline is to configure 25 megabytes of swap space for each additional ovw session that you expect to run.

Required Network Configuration

The installation starts the automatic discovery and layout of the network map, based on your internetwork's IP addressing scheme. This depends on the following:

- Correct IP addressing. The IP addresses and subnet masks must be correctly configured on the manager station, and on all routers and gateway hosts that support SNMP. Otherwise, the automatically generated map could contain incorrect networks with nodes from outside the administrative domain.
- Network design that aids isolation of network faults and traffic, by doing the following:
  - Logically subdividing an internetwork into manageable-sized networks and subnetworks, using routers, gateway hosts and IP subnet addressing.
  - Physically subdividing networks and subnetworks into manageable-sized segments using hubs, bridges, and gateway hosts. HP recommends that the segments have no more than 200 nodes each.
- SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1213) compliant agents running on management stations, routers, and gateway hosts at a minimum, and running on bridges and hubs for manageable segments. This ensures speed and accuracy of map generation.
- All HP 9000 Systems (manager stations or hosts) that are running HP-UX version 10.20 or HP-UX version 11.00 should also be running the HP OpenView SNMP Agent software as part of their networking software.
- All managed HP devices should contain a supported version of agent firmware.

Required Patches

The following patches must be installed before installing HP Hub & Switch Management for OV-UX. Contact your HP Authorized Dealer or the nearest HP Sales and Support Office, or download the patches from the HP Electronic Support Center. The URL is:

http://us-support2.external.hp.com

The two patches are:

- For HP-UX 10.20 — PHSS_15043 S700_800 10.x HP aC++ runtime library components (A.01.15)
- For HP-UX 11.00 — S700_800 11.00 HP aC++ runtime library components (A.03.10)

Before Installing HP Hub & Switch Management

Before you can begin installing HP Hub & Switch Management, you must have successfully completed installing your Network Node Manager product. See the ***HP OpenView Network Node Manager Products Installation Guide*** for instructions on installing the HP Network Node Manager and obtaining your software license.

You may set up multiple manager stations on your network. Each manager on which you install the manager product set does its own polling, so the manager traffic on your network will increase in proportion to the number of managers.

Note: This applies *only* if you buy multiple copies. Your license only entitles you to install *one* copy.

If you are installing this product set on a workstation with an existing application, be sure you first exit any `ovw` sessions currently running, then stop all HP OpenView processes using the `ovstop` command (available to root user).

Note: It is also a good practice to make a backup of your current OpenView application (especially your network map) before proceeding with the installation of new applications.

Installation Directories

The HP Hub & Switch Management product is installed in the following directories:

- `/var/opt/HPASA`
- `/opt/HPASA`

In compliance with the OSF standards, the /opt/HPASA directories hold the read-only files, which include all the executables, libraries, release notes, and Device Model Files. The /var/opt/HPASA directories contain the writeable directories such as product data directories. Be sure you have the required amount of free disk space before you install the products. You can make one of the following arrangements for the required space:

- having the required amount of disk space in `/opt` and /`var`
- mounting a dedicated volume for `/var/opt/HPASA` and `/opt/HPASA`
- making `/var/opt/HPASA` and `/opt/HPASA` symbolic links to a file system with enough disk space.

The management system must have both manager and agent software installed.

Make sure the drive that you will be loading from is connected to the workstation and that your workstation is configured to recognize the CD-ROM drive.

Consult the README file on the HP Hub & Switch Management CD for installation procedures.

Removing HP Hub & Switch Management

If necessary, you can remove products that you installed by using the command that is appropriate for your operating system. You must be logged on as root and you must remove them in the reverse order that you installed

them, that is, remove Hub & Switch Management first, then remove Network Node Manager and/or the SNMP Management Platform.

Instructions are given here for removing the Hub & Switch Management product. If you want to remove Network Node Manager, see the ***HP OpenView Network Node Manager Products Installation Guide***.

To remove products for HP-UX 10.20 or 11.00, use the HP System Administration Manager.

1. Select **Software Management**
2. Select **Remove Software**
3. Select **Remove Local Host Software**
4. Highlight the program you want to remove and pick the appropriate action from the Actions menu.

If you used the "install" command to install the software, you can also use this method for removing it:

1. Mount the Hub & Switch Management product CD in your CD-ROM drive.
2. Type in the command:

   ```
   ./remove
   ```

   This command will remove the Hub & Switch Management files and its directories. The `swinstall` command only removes the program files.

Note: The remove command only works with current Hub & Switch Management products.

Introduction to HP Hub & Switch Management

This chapter introduces HP Hub & Switch Management and includes the following topics:

HP Hub & Switch Management Overview

HP Hub & Switch Management for OV-UX is a network management application that allows you to manage and control Hewlett-Packard (HP) hubs, bridges, and switches on a TCP/IP network. HP Hub & Switch Management runs on the HP OpenView platform, which allows multivendor enterprise-wide network management. For communications with managed devices, Hub & Switch Management uses the Simple Network Management Protocol (SNMP)—an industry standard network management communications protocol.

HP Hub & Switch Management is integrated with HP OpenView Network Node Manager applications.

When using Hub & Switch Management, you can do the following:

- use HP OpenView functions to automatically discover and display the IP map (and submaps). HP hubs, bridges, and switches that are set up for SNMP/IP operation will be displayed as appropriate “connector” devices.
- use your Web browser to launch Device Views for Proactive network management
- manage HP hub and switch security features
- run network tests to troubleshoot network or device problems

HP OpenView Network Management Platform

HP OpenView is a “platform” for network management applications. As a platform, it allows multiple network management applications that are OpenView compliant—such as HP Hub & Switch Management—to share platform functionality and a common display.

Using the HP OpenView, Network Node Manager provides many shared management functions, which include:

- automatic discovery and mapping of IP networks and objects
- dynamic submap creation
- map navigation Tool Bar
- Quick Navigator
- a map zoom viewer
- device polling to monitor devices on an OpenView map
- an event notification and logging system
- generic SNMP device management
- graphing and logging of traffic
- client/server architecture enabling processes to be run on other workstations

For more information on HP OpenView platform operation and functions, refer to the HP OpenView Network Node Manager documentation.

Definitions, Processes, and Files

The basic concepts and processes of management for networks are described briefly in the following paragraphs.

SNMP Manager and Agents

HP Hub & Switch Management uses SNMP (Simple Network Management Protocol) to communicate with managed devices. SNMP commands are transmitted and received on the network using the Internet Protocol (IP).

The network management station used to run Hub & Switch Management is referred to as an SNMP **manager system**. HP devices with SNMP agents are called **agent systems**. Each network management operation requested by the manager system is executed by one or more agent systems.

The manager system communicates with HP devices to retrieve or modify management information. The devices contain Network Management SNMP Agent software to support this communication.

Note: For Hub & Switch Management operation, you must set up HP network devices for SNMP/IP operation. See Appendix A **for more information.**

Community Names for Manager and Agent Interaction

Most SNMP exchanges involve a **community name**, which can be thought of as a password for a managed device or group of devices.

Depending on the device, SNMP **get** requests for information from a device agent may require the manager to supply a community name that is configured on the device.

If a password has been specifically configured on a device, then password authentication is required to perform any SNMP **set** operations that alter the configuration or invoke self-test or reset on that device. The manager system automatically asks you for the password, then puts the encrypted password in the community name field of subsequent **set** operations.

Configuring a password on HP devices is recommended but not required. As described later in this manual, you can use Hub & Switch Management to set a device password.

What HP Devices Can Be Managed

For device management, HP Hub & Switch Management provides a Device View for most managed HP devices.

You can display a Device View using your browser if this feature is supported for the device. The devices that support this feature are noted in the table below.

Table 3-1. HP EtherTwist Devices that Can be Managed

EtherTwist Device	EtherTwist Device
HP 28688A/B EtherTwist Hub Plus (12 -port)	HP 28692A ThinLAN Hub Plus
HP 28699A EtherTwist Hub Plus/48	HP 28674B Remote Bridge RB
HP J2355A EtherTwist Hub Plus/24S	HP 28673A 10:10 LAN Bridge
HP 28682A Fiber-Optic Hub Plus	

Table 3-2. HP AdvanceStack and ProCurve Devices That Can be Managed

HP AdvanceStack Family of Hubs and Switches	HP Procurve Family of Hubs and Switches
HP J2410A AdvanceStack 100 VG Hub-15[Note 1]	HP J3288A HP ProCurve 10/100 Hub 12M[Note 5]
HP J2413A AdvanceStack 100VG Hub-7M[Note 1]	HP J3289A HP ProCurve 10/100 Hub 12M[Note 5]
HP J2415A AdvanceStack 100VG Hub-14[Note 1]	HP J3298A HP Procurve Switch 212M (**Browser-manageable**)
HP J2600A AdvanceStack 10Base-T Hub-12[Note 2]	HP J3299A HP ProCurve Switch 224M (**Browser-manageable**)
HP J2601A/B AdvanceStack 10Base-T Hub-24[Note 2]	HP J4093A HP ProCurve Switch 2424M[Note 5] (**Browser-manageable**)

Table 3-2. HP AdvanceStack and ProCurve Devices That Can be Managed

HP J2602A/B AdvanceStack 10Base-T Hub-48[Note 2]	HP J4110A HP ProCurve Switch 8000 (**Browser-manageable**)
HP J2610A/B 10Base-T Hub-8U[Note 3]	HP J4210A HP ProCurve Switch 1600 (**Browser-manageable**)
HP J2611A/B 10Base-T Hub-16U[Note3]	HP J4121A HP ProCurve Switch 4000M (**Browser-manageable**)
HP J2631A 10Base-T Hub-24 (SNMP bundle)[Note2]	HP J4122A HP ProCurve Switch 2400M (**Browser-manageable**)
HP J2632A 10Base-T Hub-48 (SNMP bundle)[Note2]	HP J4138A HP ProCurve Routing Switch 9308M[Note 5] (**Browser-manageable**)
HP J2980A AdvanceStack 10/100 LAN Switch-16[Note4]	HP J4139A HP ProCurve Routing Switch 9304M[Note 5] (**Browser-manageable**)
HP J3100A/B AdvanceStack Switch 2000 **HP J3100B is browser-manageable (firmware B.04.xx)**	
HP J3101A AdvanceStack Switch 2000 Bundle	
HP J3125A AdvanceStack Switch 200[Note 5]	
HP J3126A AdvanceStack Switch 100[Note 5]	
HP J3174A AdvanceStack Switch 208T[Note 6]	
HP J3177A AdvanceStack Switch 224T[Note 6]	
HP J3200A AdvanceStack 10Base-T Switching Hub-12R[Note 7] **Browser-manageable (firmware A.03.xx)**	
HP J3202A AdvanceStack 10Base-T Switching Hub-24R[Note 7] **Browser-manageable (firmware A.03.xx)**	
HP J3204A AdvanceStack 10Base-T Switching Hub-24T[Note 7] **Browser-manageable (firmware A.03.xx)**	
HP J3222A AdvanceStack 100Base-T Hub-12TXM[Note 8] **Browser-manageable**	
HP J3245A AdvanceStack Switch 800T **Browser-manageable (firmware B.04.xx)**	

Table 3-2. HP AdvanceStack and ProCurve Devices That Can be Managed

HP J3301A AdvanceStack 10Base-T Hub 12M **Browser-manageable (firmware A.01.xx)**	
HP J3303A AdvanceStack 10Base-T Hub 24M **Browser-manageable (firmware A.01.xx)**	

Note 1 Optional SNMP module for HP 100 VG hubs is J2414A or J2414B

Note 2 Optional SNMP module for 10Base-T hubs is J2603A/B. HP AdvanceStack 10Base-T hubs provided with SNMP module preinstalled include: HP J2630A (12-port), HP J2631A/B (24-port), HP J2632A/B (48-port).

Note 3 SNMP module J3133A available for J2610B and J2611B.

Note 4 HP J2980A 10/100 LAN Switch-16 is not supported on IPX networks. To discover this device on an IP network, the SNMP community name "public" must be configured on the device. 100VG module J2981A and 100BaseTX module J2984A available for HP J2980A.

Note 5 No IPX Network Management support.

Note 6 Requires Management Module J3178A.

Note 7 Requires Management Module J3210A.

Note 8 No Closeup View provided. Use telnet.

Note

HP AdvanceStack hubs can be chained together on a non-network connection called a Distributed Management Chain. For Hub & Switch Management to access a chain of AdvanceStack hubs, at least one hub in the chain must contain an SNMP module. Chained hubs must be of the same media type (100VG or 10Base-T). For more information, refer to the device's installation and reference manual.

For general management of generic SNMP devices (from HP and other vendors), use the HP OpenView Network Node Manager functions (such as ***SNMP Configuration*** and ***SNMP MIB Browser).***

Running HP Hub & Switch Management

This chapter describes how to start and stop HP Hub & Switch Management. It includes the following topics:

- Starting the Manager Application
- Verifying Installation of the Manager Product Set
- Stopping and Restarting the Manager Application

Note: Before you begin, you should ensure that the network devices are properly set up for IP operation. For information on setting up HP network devices, see Appendix A.

Starting the Manager Application

The entire product set that you have installed is started as one application, “the manager”, on your management station. In other words, HP Hub & Switch Management starts along with Network Node Manager.

Starting HP OpenView

Do the following steps to start your product.

1. Add `/opt/OV/bin` to your path using one of the commands below. Note that you only need to do this the first time you start the HP OpenView manager software.

For These Shells	Use These Commands
`/bin/ksh or /bin/sh`	`PATH=$PATH:/opt/OV/bin:/usr/sbin` `export PATH`
`/bin/csh`	`setenv PATH “$PATH:/opt/OV/bin:/usr/sbin”`

2. Optionally, execute the `/opt/OV/bin/ovstatus` command to verify that the trapd, ovwdb, ovtopmd, and netmon background processes are running. If the background processes are not running, execute the `/opt/OV/bin/ovstart` command. If you are surprised that a background process is not running, run `ovstart -v`, which gives you more information. The `ovstart` command starts the background processes. (You must be root to perform this step.)
3. If you are not running X Windows (X Windows, HP VUE or HP CDE for HP-UX systems), start it.
4. Optionally, if you want to redirect your X Windows display to a system other than the management system:
   a. Set your X Windows DISPLAY variable on the HP OpenView network management system using one of the commands below. Replace ***hostname*** with the host name of the system to which you are redirecting the display.

For these shells	Use these commands
`/bin/ksh` or `/bin/sh`	`DISPLAY=hostname:0.0` `export DISPLAY`
`/bin/csh`	`setenv DISPLAY hostname:0.0`

5. Make sure that the management system has permission to display windows on ***hostname***. If the management system does not have permission, and if the hostname is using the host-based authorization, use the xhost command to add the management system to the xhost table on the ***hostname*** system. To do so, on ***hostname*** type:

   ```
   xhost + <managementsystem name>
   ```

   where ***managementsystem*** name is the host name of the management system. If the hostname is using the MIT-MAGIC-COOKIE-1 authorization, please refer to the xauth man pages to set up the .Xauthority file.
6. Start the graphical network map (user interface) by typing:

   ```
   ovw
   ```

   ovw is executable by anyone.

   Alternatively, you can run `ovw` in the background to free up the terminal window for other uses. In some cases, ovw prints error messages to standard output and standard error. To capture these messages and to

prevent jobs from stopping, you may want to redirect messages to a temporary file. To run `ovw` in the background and to redirect error messages to a temporary file, type

```
ovw > /tmp/ovw.log 2>&1 &
```

This starts up the entire product set you have installed. The graphical network map will be generated in a window, with the HP Hub & Switch Management menu items available in the pull-down menus from the menu bar.

For more information, refer to the ***HP OpenView Network Node Manager Reference*** and the various **man** pages on the processes.

Verifying Installation of the Manager Product Set

If the products are installed properly, you should find the menu items associated with HP hubs, bridges, and switches under the “Options” and “Monitor” menus. The Menu items that Hub & Switch Management adds to Network Node Manager are shown in the following table.

Table 4-1. OpenView Menu Items

OpenView Menu	Menu Item added by HP Hub & Switch Management	Description
Monitor	HP Hub/Switch	**Monitor HP Hub/Switch**: Displays a graphical control panel (Closeup View) of a selected (IP-addressed) HP hub, bridge, or switch. **SNMP Configuration**: Allows you to configure the following on the devices that can be managed with a browser: Thresholds Trap Receivers Community Names Authorized Managers

Table 4-1. OpenView Menu Items

OpenView Menu	Menu Item added by HP Hub & Switch Management	Description
Options	HP Hub & Switch Admin	Runs the HP Admin utility for setting Hub & Switch Management parameters.

Note: For information on setting up network devices for IP operation, see Appendix A**.**

Stopping and Restarting the Manager Application

Stopping the Manager

Stopping the manager consists of:

1. Exiting the manager's graphical network map and user interface, and
2. Optionally stopping the manager's background processes.

To exit from the network map and interface (ovw), select **Exit** in the map's **File** menu.

If you want the manager to continuously collect data and monitor changes even when the map and interface are not up (that is, even if you exit from ovw), do step 1 and ***not*** step 2. The background processes—netmon, trapd, ovwdb, ovtopmd, and snmpCollect—will continue to run and you need only run `/opt/OV/bin/ovw` to return to the map and interface. For more information on these background processes, refer to the ***HP OpenView Network Node Manager Reference*** manual or read the **man** page for the process.

If you want to stop the background processes, use the command `/opt/OV/bin/ovstop`. Using `ovstop` without arguments stops all of the processes—netmon, trapd, ovwdb, ovtopmd, and snmpCollect—in the correct order.

Restarting the Manager

If you have stopped the background processes and you want to restart them, use the command `/opt/OV/bin/ovstart`.

5

Alerts - Find/Fix/Inform

This chapter contains information on:

HP Proactive Networking

HP Proactive Networking offers the combined benefits of outstanding products and effective, easy-to-use network management that provide you with the control, uptime and performance your network needs.

Note: Devices that are manageable with your Web browser feature HP Proactive Networking. For older HP devices, read the chapter "Management for Non-Browserable Devices" or see the online help.

Control

Control with Management. Improve control of your network with:

- Increased visibility into the network by monitoring all segments and displaying network performance information
- Compatibility with other vendor's products

Control with Technologies. For your future network, you will need to rely on emerging technologies. Two principal emerging technologies that HP provides are:

- **Gigabit Ethernet.** This technology is the natural evolution of 10Base-T and 100Base-T. It is the high-performance network of the future.

- **Advanced Switching.** New switching techniques like meshing, VLAN tagging, and voice and data handling provide high performance networking for the future.

Control of Costs. HP provides Total Cost of Ownership benefits by focusing on "out-of-the-box" manageability based on a combination of HP Top Tools for Hubs & Switches and management-enabled hardware.

Uptime

Find, Fix, Inform. The Find/Fix/Inform feature of HP Proactive Networking discovers, corrects, and reports on problems that occur on the network. The three parts are:

- **Hardware Agent.** The hardware agent monitors the network continuously, automatically balancing traffic and finding and fixing most common network problems.
- **Management Software.** The Web browser-based user interface provides a consistent, friendly environment for monitoring your network.
- **Network Manager.** HP Hub and Switch Management for OV-UX helps you achieve maximum control, uptime, and performance by letting you manage the network anytime, anywhere.

Quality and Reliability. High quality, reliable HP products will help keep your network running into the next century. HP's Quality of Service provides service-level guarantees for mission critical applications and multimedia communication applications.

Best Warranty and Support. HP products are backed by a lifetime warranty (for as long as you own the product) and free end-user telephone support. Every HP Proactive Networking product is Year 2000 ready.

Performance

Bandwidth Performance. Video and multimedia applications require large amounts of bandwidth. HP has these solutions to meet your bandwidth needs:

- A line of high-speed hubs and switches that deliver extensive bandwidth to the desktop. HP hubs and switches use industry-standard Ethernet technology with its low cost and scalability from 10 Mbps to 1,000 Mbps.
- Protocols and product software that control bandwidth utilization and improve information delivery
- Backbones that are fast, reliable and robust

- Switch meshing for switching
- Cisco Fast EtherChannel® for servers

HP Proactive Networking products save time, money and increase productivity.

Interpreting the Alert Log - Find/Fix/ Inform

The Alert Log is displayed in the lower area of the device's Status - Overview page. Its "Find/Fix/ Inform" (patent pending) capability helps you proactively manage your network by displaying device traps and problem conditions in one easily accessible browser page. It displays messages about events that have occurred on the device, such as loss of link, a problem cable, or a broadcast storm. Select **Open Event** or double-click on an alert to display more information.

The dialog box displays more information about the alert as well as some suggestions for fixing the problem. When you have reviewed an alert, the "New" icon is no longer displayed. Closing an alert indicates that it is no longer a problem.

The following table shows the common faults and how they are indicated.

Table 5-1. Find/Fix/Inform Faults

Problem	How the Problem is Indicated
Fault 1: Problem Driver or Network Interface Card (NIC)	Indicated by long or short packets with good CRCs.
Fault 2: Problem XCVR or NIC	Indicated by long packets with bad CRCs.
Fault 3: Problem Cable	Indicated by normal size packets with CRC errors.
Fault 4. Cable Length/Repeater Hops	Indicated by late collisions.
Fault 5: Over Bandwidth	Indicated by a high collision rate.
Fault 6: Broadcast Storm	Indicated by a high rate of broadcast packets.

Table 5-1. Find/Fix/Inform Faults

Problem	How the Problem is Indicated
Fault 7: Auto Partition (hubs only)	Indicated by a port repeatedly partitioning and healing due to a network loop or problem cable.
Fault 8: Misconfigured SQE (hub only)	Indicates a misconfigured transceiver detected by internal hardware.
Fault 9: Polarity reversal (hub only)	Indicates a mis-wired cable detected by internal hardware.
Fault 10: Network Loops	Indicated by a high traffic level in correlation with duplicate traffic on the network.
Fault 11: Link Loss	Lost link beat to a cascade port.

The Find/Fix/Inform function runs continuously in the background at a sensitivity threshold level that you select. Sensitivity threshold settings control the severity of the alerts that are displayed. The settings internally adjust the counter thresholds automatically.

Sensitivity settings are selected in the Configuration page for the device. Select the **Fault Detection** button. For hubs, you can set the sensitivity for logging network problems and disabling ports. Switches only have a sensitivity setting for logging network problems. Switches are more capable of isolating problems occurring on a single port than hubs are.

The sensitivity settings are:

- **High Sensitivity**: the device will act when a network problem of any severity occurs. Network problems are automatically detected and entered into the Alert Log (located under the Status Tab).
- **Medium Sensitivity**: the device will act when serious network problems occur.
- **Low Sensitivity**: the device will act only when severe network problems occur. These are problems that may bring the network down.
- **Never**: The device will never take any actions regardless of the severity of the problem.

Only serious and persistent problems that impact other users on the network will cause a hub to disable a port. These problems include:

- A problem XCVR or NIC
- A broadcast storm
- Excessive Auto Partitions
- A network loop

- Full/Half-duplex mismatch

A warning is entered in the Alert Log shortly before the port is disabled. Another entry is made indicating that the port has been disabled.

Acknowledging Events. Click on the **Acknowledge Selected Events** button to indicate that you have seen the alert. Acknowledging an alert changes its state from *new* to *open*.

Closing Events. To close an alert and remove it from the Alert Log, select the alert and click on the **Close Events** button.

Sorting Events. Double-click on the column head to sort the alerts according to severity, the name of the alert, the address of the device, or the date and time of the alert.

Deleting Events. Click on the **Delete Selected Events** button to remove these alerts from the Alert Log.

First Time Installation Information. There will be an entry in the Alert Log for first time installation information for the device.

6

Accessing Hub Features

HP Hub & Switch Management lets you manage your HP devices with your browser from anywhere in your network. Several features provide information about the status of your device, alert you to problems in your network, and give you the ability to configure settings for proactive network management.

Note: For older HP devices that cannot be managed with a Web browser, read the chapter "Management for Non-Browserable Devices" or see the online help.

This section includes information on:

- Accessing the Device View
- Viewing Device Identity Information
- Interpreting Device Status
- Reading the Performance Gauges
- Status - Global Counters
- Configuring Your Device
- Fault Detection
- Load Balancing
- Support

More Information on Device Features

See Setting Up Security for a Device for information about device security.

See Performing Diagnostics for information about resetting devices and performing Link and Ping tests.

Accessing the Device View

To launch the Device View, double-click on a device symbol in the HP Network Node Manager map or right-mouse-click on the device symbol and select **Monitor HP Hub/Switch**. The Status - Overview page for the device displays. Select the **Configuration** tab and click on **Device View** to display the port view of the device.

Viewing Device Identity Information

You can view some basic information about the device by selecting the **Identity** tab. You can change the information by selecting the Configuration tab and clicking on the **System Information** button.

See the online help for information about setting or changing these values.

Interpreting Device Status

The Status - Overview page for the hubs displays the Performance Gauges and any alerts that have occurred. For switching hubs, the Status - Overview page displays gauges by segment instead of by attribute.

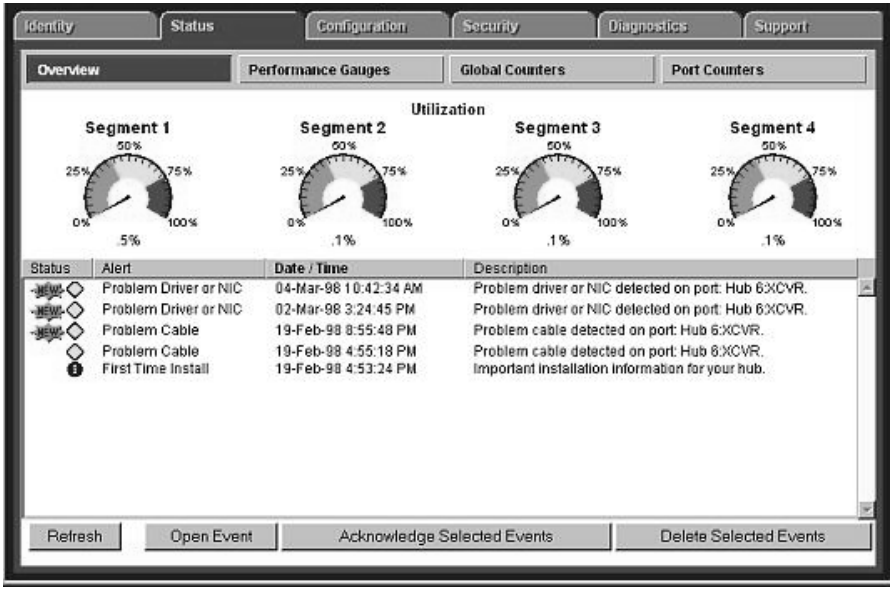

Figure 6-1. Segmented Hub Status Overview Page

Reading the Performance Gauges

The performance gauges display statistical information about the selected device. By looking at the gauges, you can quickly determine if there are problems with the network utilization, collisions, the number of broadcasts per second, or the number of error packets. The gauges are refreshed every five seconds.

The information shown for hubs is for all ports on the device. You can obtain information for each port by selecting the Performance Gauges button, then selecting an individual port from the drop down list. If you want to monitor a different attribute for that port, just select the desired attribute from the drop down list below the port number.

The following table explains the attributes and gives their threshold settings on a per port basis for hubs. These settings cannot be changed. You can view an attribute value for all the ports of a device by selecting **All Ports** from the drop down list above the attribute. For the switching hubs, you can also select a segment from the drop down list.

Table 6-1. Gauge Attributes for Hubs

Attribute	Description	Severity Values
Utilization%	Represents the traffic on the port as a percentage of the port's bandwidth.	Warning: 40% Critical: 75%
Collisions%	Represents the number of collisions that have occurred expressed as a percentage of the packets transmitted through the port.	Warning: 30% Critical: 50%
Broadcasts/sec	Represents the number of broadcast packets being transmitted through the port per second.	Warning: 150/sec Critical: 400/sec
Errors%	Represents the number of errors that have occurred expressed as a percentage of the total number of packets received through the port.	Warning: 0%-1% Critical: 1%
Multicasts/sec	Represents the number of multicast packets being transmitted through the port per second.	Warning: 1500/ sec Critical: 4000/sec

Status - Global Counters

Hub Global Counters

Selecting the Global Counters button displays a page listing eight counters and their values since the last device reset. The counters are totals for the device. To view counters by port, select the Port Counters tab.

Switching Hub Global Counters

The switching hubs display the counters described in the following table.

Table 6-2. Switching Hub Global Counters

Counter	Description
Total Packets	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Table 6-2. Switching Hub Global Counters

Counter	Description
Total Octets	Total number of octets of data (including bad packets) received on the network. This object can be used to estimate Ethernet utilization.
Broadcast Packets	Messages sent to all users on the network.
Multicast Packets	Multicast packets are delivered to a subset of users on the network, as opposed to Broadcast packets, which are sent to all users.
Collisions	When two or more devices attempt to transmit a message on a cable at the same time, interfering with one another's transmissions. The number of collisions should be proportional to the number of packets transmitted over time and the number of nodes operating on the network.
CRC/Alignment Errors	The Cyclic Redundancy Check (CRC) is a code typically placed at the end of the frame or packet to ensure the integrity of the data within the frame. Alignment Errors are the number of instances where the CRC method was used to correct a packet whose bits were misaligned because of timing errors.
Fragments	Total number of packets received that were less than 64 octets in length and had a bad Frame Check Sequence (FCS).
Jabbers	Total number of packets received that were longer than 1518 octets and had a bad Frame Check Sequence (FCS). High levels indicate too many packet transmissions.

Status - Port Counters

The Port Counters button displays a page with information about important counters for each port. See the online help for information on each counter.

Configuring Your Device

When you select the Configuration tab the Device View (formerly a Closeup View) is displayed in the page. The other buttons in this page provide access to various configuration features for that device.

If the device you selected is not manageable by browser, you can only manage it from the management workstation.

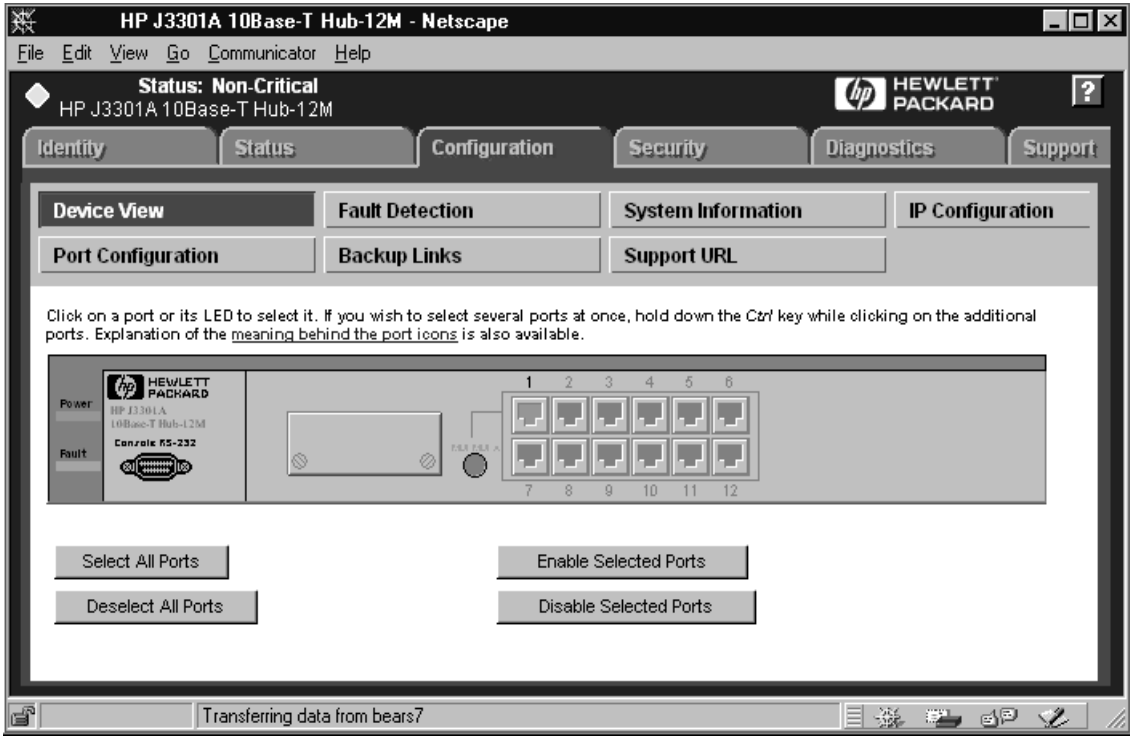

Figure 6-2. 10Base-T Hub-12M Device View

You can enable and disable individual ports (click on the port to select it), or click on the **Select All Ports** button to enable or disable all the ports of a device in one step.

For the switching hub, select a hub or card from the stack using the drop down list at the top. The Closeup View for that hub or card will display.

To move selected ports to a particular segment:

1. Select the **Move Selected Ports to Segment** button.
2. Select a hub from the drop down list, then select the segment that you want to move the port to.
3. Click on **Apply Settings**.

Click on the link “meaning behind the port icons” to view the port indicator legend.

Configuration - Fault Detection

The automatic fault detection feature protects your network from failing because of problems such as network loops, defective cables, transceivers and faulty network interface cards. The Fault Detection page lets you set the sensitivity and actions that occur when a fault is detected on a port in your network. For hubs, you can set the sensitivity for logging network problems and disabling ports. The sensitivity settings are:

High Sensitivity: the device will act when a network problem of any severity occurs. Network problems are automatically detected and entered into the Alert Log.

Medium Sensitivity: the device will act when serious network problems occur.

Low Sensitivity: the device will act only when severe network problems occur. These are problems that may bring the network down.

Never: The device will never take any actions regardless of the severity of the problem.

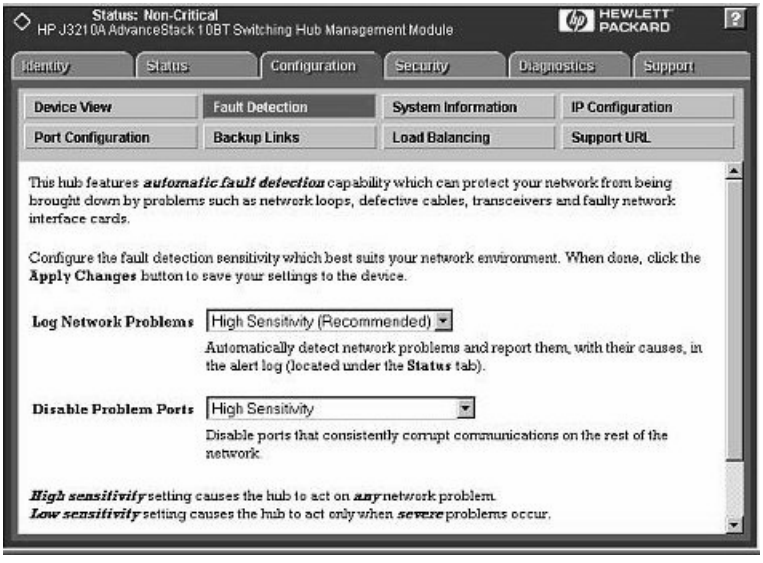

Figure 6-3. Fault Detection Sensitivity Settings

Configuration - System Information

The System Information page lets you enter a system name for the device, the location of the device, and whom to contact in the event of a problem.

Configuring IP

Select the way that you want IP addresses configured for your network:

- Manual - Set the IP address through the console.
- Disabled - IP is disabled, there is no access to management or telnet. **Not Recommended**.
- Use Bootp - The Bootp protocol sets the IP address automatically.

Hub IP Configuration

If you select Manual, you must then enter an IP Address, Subnet Mask, Default Gateway, and Time to Live for the device. If you select Bootp/DHCP, the IP address will be assigned automatically.

Switching Hub IP Configuration

For the switching hubs, you must select a segment to configure before you select Manual or Bootp/DHCP. If you select Manual, you must then enter an IP Address, Subnet Mask, Default Gateway, and Time to Live for the device. If you select Bootp/DHCP, the IP address will be assigned automatically.

Characteristics of Bootp and DCHP. The Bootp protocol is designed for a network in which each host has a permanent network connection. It is not adaptable to a mobile computing environment.

The Dynamic Host Configuration Protocol (DHCP) manages the allocation of TCP/IP configuration information by automatically assigning IP addresses.When a device connects to the network, it requests an address from the DHCP server. In dynamic mode, the address is used by the device for a specified period of time. The time period depends on the situation; one device may only need the address for an hour, while another device may use the same address for several days. DHCP is more suitable in environments where the number of IP addresses needed exceeds the number available. It also allows a device to obtain its configuration information, such as the IP Address and Subnet Mask, in one message, reducing the demand on the network.

A static IP address is a unique address that is assigned to one client only. Static addresses are used for an extended time period.

Port Configuration

The Port Configuration page displays information about the hub ports. To enable a port, select the port number in the page, then click **Enable Selected Ports**. Use the **Disable Selected Ports** button to disable a port or group of ports.

The information displayed is described in the table.

Table 6-3. Hub Port Configuration

Setting	Description
Port	The port number.
State	The port can be on or off.
Connected	**Yes**: A device is connected to this port. **No**: There is nothing connected to this port. **Partitioned**: The node is disconnected from the network and the traffic that the port generates is lost. **Polarity Reversed**: Some signals in the cable are reversed due to a miswired cable.
Segment	For switching hubs, the segment that the port is on.
Last Source Address	The address of the last device that sent packets through this port.
Security Violation	States whether there is a security violation or no violation.

Configuration - Backup Links

A backup link (hubs only) configures two ports on one hub to create a redundant connection to another device. This provides a connection with fault-tolerant capability for highly reliable networking. One port is designated the primary port; the second port is the backup port. The backup port becomes active only if the primary port becomes inoperative. Any of the

network ports (twisted-pair, ThinLAN, or AUI/Xcvr) can be used as the primary port or backup port.

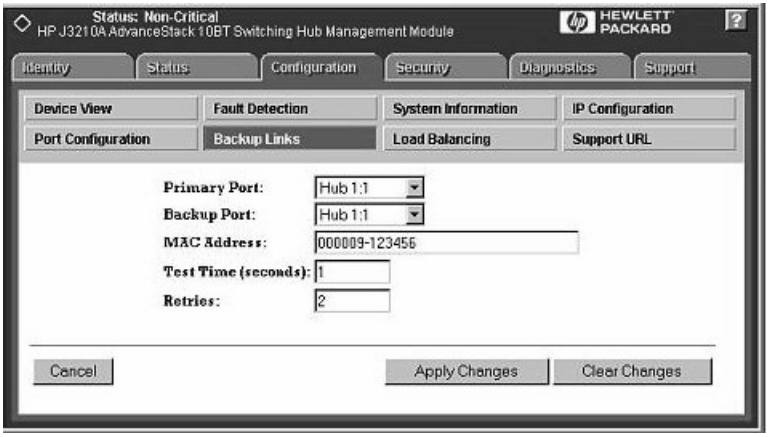

Figure 6-4. Setting Backup Links

You can create one or more backup links by selecting the **Backup Links** button and clicking on the **Add New Backup Link...** button at the bottom of that page. The parameters are described in the table.

Table 6-4. Backup Link Parameters

Parameter	Description
Status	Displays which port is currently being used, a primary port or a backup port.
Primary Port	A port that you can use as a primary port, or the port that will be used during standard connection of a hub and the connected device.
Backup Port	The backup port to be used if there is a failure on the primary port.
MAC Address	The MAC address of the device that the primary and backup ports are connected to.

Table 6-4. Backup Link Parameters

Parameter	Description
Test Time	The interval in seconds between test packets sent between the primary port and the receiving device.This checks the integrity of the link to determine whether to initiate a backup link.
Retries	The maximum number of times the primary port can fail before the backup port becomes active.

Configuring Load Balancing - Switching Hubs

Only the switching hubs provide a load balancing feature to automatically distribute the switching hub ports among the four segments to optimize performance. For switching hubs with version A.01.01 firmware this feature requires a switch module. For switching hubs with firmware versions later than A.01.01, the hub can load balance with an external switch.

To access this feature, select the **Load Balancing** button. Click on the **Perform Automatic Load Balancing** button. If you want to undo the load balancing, select the **Undo Last Load Balancing** button.

Configuration - Support URL

You can obtain support information by going to the HP Support site on the World Wide Web. The URL is:

http://www.hp.com/go/procurve

Select **Support**.

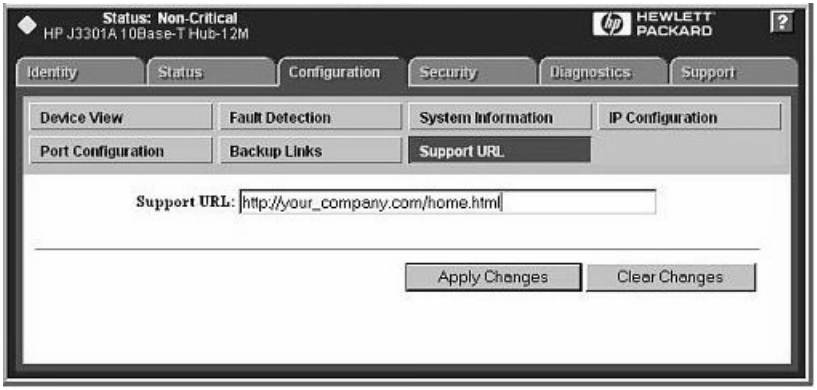

Figure 6-5. Support URL

If you want to change the URL that is accessed when the Support tab is selected, type in the new address and click on the **Apply Changes** button. For example, you could change the URL to launch your site home page.

7

Managing Switches

This chapter has information on:

- Switch Status
- Switch Identity
- Configuration
- Using VLANs
- Support/Mgmt URL

Switch Status

Status - Overview

To launch the Status - Overview page for a switch that is manageable by browser, double-click on the switch symbol in the HP Network Node Manager map or right-mouse-click on the symbol and select **Monitor HP Hub/Switch**.

Note: If the device is not manageable by browser you will see the Closeup View in a separate window (you must launch the Closeup View from the management station). Read the chapter "Management for Non-Browserable Devices" or see the online help for more information.

The Status - Overview page is divided into two areas, the Graph area and the Alert Log area.

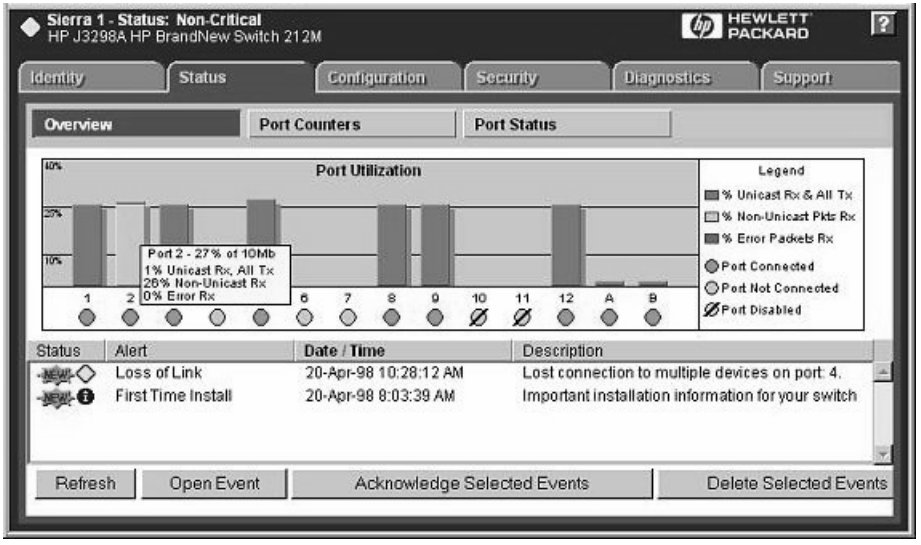

Figure 7-1. Switch Status Overview Page

Graph Area

The bar graph gives a quick overview of the performance of the switch. Each bar shows the highest percentage of transmitted (TX) or received (RX) traffic utilization for that port in the last five seconds.

The graph area proportionally depicts three attributes for each port:

- Unicast packets - The percent utilization for packets that were not addressed to a multicast or broadcast address.
- Non-Unicast packets - The percent utilization of received non-unicast packets (both broadcast and multicast). If there is a broadcast storm, only the port receiving these packets shows high utilization, letting you quickly pinpoint the problem.
- Errors - The percent utilization for error packets received. A high percentage may indicate possible network problems.

Place the cursor over a bar in the graph to display the exact percentages for each attribute and the speed of that port. The above graph displays a high percentage of non-unicast packets on port 2 (a 10 Mbps port) because this port is running video. Port 5 is indicating some errors.

The graph only scales to 40% utilization. Network utilization above this level indicates serious performance problems.

The graph also shows you if a port is active, disabled, or not connected.

Alert Log Area - Find/Fix/Inform

The “Find/Fix/Inform” capability of a device helps you proactively manage your network by displaying traps sent from the device in an easily accessible browser page. The device monitors counters and internal hardware information. When a problem is discovered, such as loss of link, a problem cable, or a broadcast storm, the Alert Log displays clear messages about the problem. When you double-click on an alert in the Alert Log (or select the alert and click on the Open Event button), the Alerts page displays more information about the alert as well as some suggestions for fixing the problem.

For example, the Alert Log may display the alert “Cable Length”. The following information is available:

Description:

Packet loss detected on port 4. This may be due to an overextended LAN topology or faulty hardware. The loss was detected on this port, but the actual problem can be occurring elsewhere on this segment.

Solution:

- Verify the network topology is within IEEE 802.3 topology standards. All ThinLan coaxial cabling must be 185 meters or shorter. No more than 4 repeaters are allowed between any two stations in the network.
- Insert bridges or switches between repeaters to extend network topology if needed.
- Check for faulty cabling, transceivers, and NICs.
- Check for a Full/Half-duplex mismatch

Using the Find/Fix/Inform capability, the device can isolate a problem that occurs on one port, preventing it from affecting the entire network.

See Alerts - Find/Fix/Inform for information on reading and acknowledging alerts.

Status - Port Counters

The Port Counters information for switches displays specific network conditions or traffic. See the online help for more information about each counter.

Status - Port Status

The Port Status page (switches only) displays the operational status of each switch port. The settings can be changed in the Configuration - Port Configuration page.

The Port Status settings are described in the following table.

Table 7-1. Port Status Settings

Setting	Description
Port	The port number.
Port Type	The network type of each switch port, for example, 100TX.
Enabled	Whether the port is enabled or disabled.
Link Status	The port's current operational status. Up means the port is working correctly. Down means the port is disabled.
Current Mode	The operational mode of the port. • 10/100 Base TX - Can be 10 Mbits half or full duplex or 100 Mbits half or full duplex. • 100 Base FX - Can be 100/full duplex or 100/half duplex. • Gigabit - Can only be 1000 full duplex.
Flow Control	Indicates the current state of flow control for this port. • 10/100TX, 10 FL, 100 FX: – On - Flow control is enabled. – Off - Flow control is disabled (default). • Gigabit: – On (TX, RX) - Flow control is enabled on transmit and receive. – On (RX) - Flow control on receive only. – Off (default) - Flow control is disabled.

Table 7-1. Port Status Settings

Setting	Description
Bcast Limit (not available on the HP J3298 A or HP J3299A)	The Broadcast Limit, expressed as a percentage of broadcast packets relative to the theoretical limit. Any broadcast or multicast traffic exceeding this limit will be dropped. A value of zero indicates that no limit is to be applied. Values range from 0-99.

Identity

The Identity tab displays the following information about the switch:.

- System Name
- System Location
- System Contact
- System Up-Time
- Product Number and Name
- Firmware Version
- IP Address
- Management Server

The Management Server field displays the address (URL) of the management station where HP Hub & Switch Management was installed. This can be changed by selecting the Configuration tab and displaying the **Support/ Mgmt URLs** page. Enter the URL in the Management Server URL field. Online help can be displayed at any client when this URL is set correctly.

Configuration

The Configuration page lets you configure many device features, for example, the sensitivity levels for Fault Detection.

Device View

There is a Device View for every managed HP switch. The Device View for the HP ProCurve Switch 4000M looks like the following graphic. Use the online help to obtain information about specific switch modules.

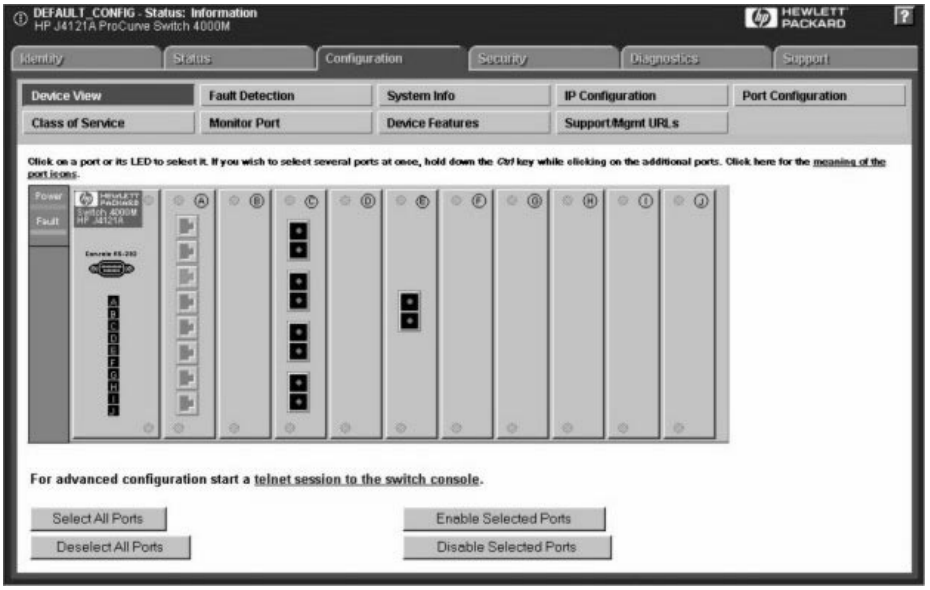

Figure 7-2. HP ProCurve Switch 4000M Device View

Configuration - Fault Detection

The automatic fault detection feature protects your network from failing because of problems such as network loops, defective cables, transceivers and faulty network interface cards. Network problems are automatically detected and entered in the Alert Log. The Fault Detection page lets you set the sensitivity levels for the actions to be taken when a fault is detected on a port in your network. Switches only have a sensitivity setting for logging network problems. The sensitivity settings are:

High Sensitivity: The device will make an entry in the Alert Log (located in the Status tab) when a network problem of any severity occurs.

Medium Sensitivity: The device will make an entry in the Alert Log when serious network problems occur.

Low Sensitivity: The device will make an entry in the Alert Log only when severe network problems occur. These are problems that may bring the network down.

Never: The device will never make any entries in the Alert Log regardless of the severity of the problem.

Configuration - System Information

The System Information page lets you enter a system name for the device, the location of the device, and whom to contact in the event of a problem.

Configuration - IP Configuration

Select the way that you want IP addresses configured for your network:

- Manual - Set the IP address through the console.
- Disabled - IP is disabled, there is no access to management or telnet. **Not Recommended**.
- Use Bootp - The Bootp (or DHCP) protocol sets the IP address automatically.

If you select Manual configuration, you can change the IP address, a subnet mask, and a default gateway for the device.

Some switches let you configure an IP address for every VLAN you have created.

Figure 7-3. Switch IP Configuration

Characteristics of Bootp and DHCP. The Bootp protocol is designed for a network in which each host has a permanent network location. It is not adaptable to a mobile computing environment.

The Dynamic Host Configuration Protocol (DHCP) manages the allocation of TCP/IP configuration information by automatically assigning IP addresses.When a device connects to the network, it requests an address from the DHCP server. In dynamic mode, the address is used by the device for a specified period of time. The time period depends on the situation; one device may only need the address for an hour, while another device may use the same address for several days. DHCP is more suitable in environments where the number of IP addresses needed exceeds the number available. It also allows a device to obtain its configuration information, such as the IP Address and Subnet Mask, in one message, reducing the demand on the network.

A static IP address is a unique address that is assigned to one client only. Static addresses are used for an extended time period.

Configuration - Port Configuration

The Port Configuration page displays information about the switch ports. The settings are explained in the following table. To modify a port setting, click on a port then select the **Modify Selected Ports** button. Modify multiple ports at one time by using Ctrl-Click to select the desired ports.

Note: Some switches support trunking. For information on trunking, see the online help for that device.

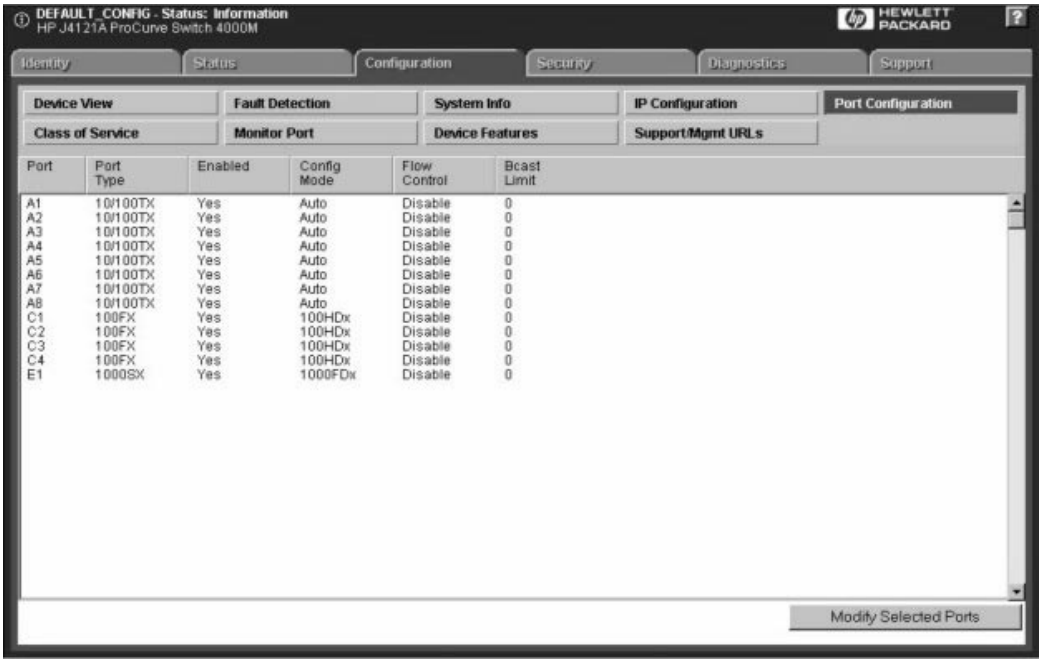

Figure 7-4. Switch Port Configuration

Table 7-2. Switch Port Configuration Settings

Setting	Description
Port	The port number. The port may be appended with one of the following: • Trkx - The port trunk to which this port belongs • Mesh - The port has been assigned to a switch mesh domain • MP - The port is a Monitor Port
Port Type	The MAC layer type, for example, 100VG or FDDI.
Enabled	Whether the port is enabled or disabled.
Config Mode	The speed and duplexing for the port. Auto mode will negotiate with the device on that port to determine the mode. Click on **Modify Selected Ports** to change the mode.
Flow Control	Indicates the current state of flow control for this port. When disabled, the port does not generate flow control packets and drops any flow control packets it receives. • 10/100TX, 10FL, 100FX: – On - Flow control is enabled. – Off - Flow control is disabled (default). • Gigabit: – On (TX, RX) - Flow control is enabled on transmit and receive. – On (RX) - Flow control on receive only. – Off (default) - Flow control is disabled.
Bcast Limit	The Broadcast Limit, expressed as a percentage of broadcast packets relative to the theoretical limit. Any broadcast or multicast traffic exceeding this limit will be dropped. A value of zero indicates that no limit is to be applied. Values range from 0-99.

Configuration - Assigning a Monitoring Port

The Monitor Port tab (only found on switches) lets you select a “Monitoring Port” that you can use with a network analyzer to monitor other ports on the switch. For the HP J3298A and HP J3299A you can only choose the Monitoring port and the port to be monitored. For other switches you can choose to have all the ports for one VLAN monitored, or you can select individual ports to be monitored. See the online help for information on specific switches.

Figure 7-5. Selecting a Monitoring Port on a Switch

Using VLANS

Virtual LANs, or VLANs, are generally defined as broadcast domains created with software rather than being a function of the hardware. They can be viewed as a group of end nodes, possibly on different physical LAN segments, that can communicate with each other.

As networks expand, more routers are needed to separate users into broadcast domains. Latency degrades network performance, and is a special problem for multimedia applications. Switches using VLANS create the same division of the network into broadcast domains, but do not have the latency problems of a router. Switches are also a more cost-effective solution. You can create virtual LANs by assigning selected ports of your HP switch to a VLAN.

The benefits of VLANs include:

- Grouping users into logical networks for increased performance

- Providing an easy, flexible, less costly way to modify logical groups in changing environments
- Preserving current investment in equipment and cabling
- Allowing administrators to “fine tune” the network
- Providing independence from the physical topology of the network

VLANs make large networks more manageable. You can group users according to some shared characteristic, such as a common business function or a common protocol. A single switch may have several independent VLANs within it.

Note: VLANs must be created with the device console.

Configuration - Device Features

The Device Features page (only found on switches) lets you set some or all of these features:

- Automatic Broadcast Control (ABC)
- Multicast Filtering (IGMP)
- Spanning Tree

Automatic Broadcast Control (ABC)

Automatic Broadcast Control (ABC) is a feature that controls broadcasts through IP/IPX Broadcast Reduction. IP/IPX Broadcast Reduction reduces the number of broadcasts propagated through the network.

Using ABC, the switch acts as a proxy server, replying to Address Resolution Protocol (ARP) requests, Nearest Server Query (NSQ) requests, and GetLocalTarget requests on behalf of the destination node. An ARP cache (learned address table) is created for each subnet allowing the switch to proxy reply with the resolved MAC address instead of forwarding the requests out all ports. This limits the broadcasts within the switching domain. The Service Advertising Protocol (SAP) table performs the same function in an IPX network. By using these tables, the switch can resolve addresses for any node in the network that it already knows about.

Routing Information Protocol. The switch also intercepts Routing Information Protocol (RIP) and SAP broadcasts and forwards these only to ports where routers and servers have been detected. This also reduces the number of broadcasts on the network.

For example, if User A sends out a broadcast message to connect to its server, the request is sent out of all ports on the switch. When the server responds to User A, the switch intercepts the response and learns that the server is on that port. When User B sends a request to the same server, the switch already knows which port that server is on and sends that information to User B, just as if the server had responded to the request. User B's request is not broadcast out any of the switch ports.

Enabling Broadcast Control for IP

The IP protocol uses Address Resolution Protocol (ARP) packets to find the MAC address of a node that corresponds to the network layer address. When Broadcast Control is enabled, the switch intercepts the ARP packet on its way to the destination node. If this destination is unknown to the switch, the switch floods the ARP request to all ports. When the destination port responds, the switch stores information about the destination MAC address and layer 3 address in its ARP cache. This information allows the switch to proxy a reply containing the MAC address of a destination to the source of an ARP request. The source can then send a unicast packet directly to the destination. The amount of broadcast traffic has been decreased.

Automatic IP RIP Control. To further reduce broadcast traffic, you can check Automatic IP RIP Control. IP RIP packets are sent out periodically (every 30 seconds) to distribute routing information. By enabling Automatic IP RIP Control, the switch will only forward RIP packets out the ports on which RIP packets have been received. Since routers are the only devices that generate RIP packets, this ensures that RIP packets are only sent out ports with routers attached to them. When this feature is not enabled, IP RIP packets are forwarded to all ports.

Enabling Broadcast Control for IPX

The IPX protocol broadcasts all of its known routes and services every minute by using IPX, RIP and Service Advertising Protocol (SAP) packets. When servers are booted up, they advertise their services using SAP. These frames must be forwarded by routers, which maintain a database of this information, allowing clients on the network to obtain the internetwork addresses of the servers where they can access services.

Automatic IPX RIP/SAP Control. To further reduce network traffic, you can check the Automatic IPX RIP/SAP Control check box. The switch will intercept RIPs and SAPs, broadcasting them only to ports where IPX routers or servers have been detected, or to ports that have been configured to

transmit RIPs or SAPs. When this feature is not enabled, IPX RIP/SAP packets are forwarded to all ports.

Automatic IP Gateway Configuration

When Automatic IP Gateway Configuration is enabled, the switch will modify replies from the DHCP server so that the Default Gateway IP address of a client becomes the client's own IP address. This is useful in a multinetted environment (where more than one IP network is configured in a single broadcast domain).

See Routing Information Protocol.

Internet Group Management Protocol (IGMP)

Multimedia and email applications need the ability to communicate to multiple destinations efficiently. IP multicasting allows hosts to dynamically register for sending or receiving multicast traffic.

The Internet Group Management Protocol is a method for automatically controlling multicast traffic through the network. Using multicasting, applications can send one copy of a packet addressed to a group of computers that wish to receive it. This method is more efficient than sending a separate copy to each node. Other advantages of multicasting include:

- information delivered in a timely, synchronized manner because all destination nodes receive the same packet
- information can be sent to destinations whose addresses are unknown
- reduces the number of packets on the network because only one multicast packet is sent.

IGMP uses multicast queriers and hosts that support IGMP to manage multicast traffic on the network. It specifies how the host informs the network that it is a member of a multicast group. A set of queriers and hosts that send and receive data from the same set of sources is a multicast group.

The HP switches have a standards-based IGMP implementation. The switches process IGMP packets by learning which of the switch's interfaces are linked to hosts that are members of multicast groups and multicast routers. It limits multicast traffic by monitoring the IGMP traffic to learn which hosts are in which multicast groups, then allowing IP multicast traffic to be sent only to ports with valid host group members.

When a switch receives an IGMP packet, it updates the internal IP multicast forwarding table with the IGMP membership read from that packet. The

switch then sends the packet to the ports with members of the destination multicast group.

Special multicast routers/queriers communicate by using three message types - query, report, and leave group. The query message, sent by a querier, is used to discover which network interfaces belong to a multicast group. Each host responds to the query message with a report message that tells the querier the host is a member of the multicast group. The host also can send a report message to join a group or a leave message to leave a group.

Note: Using the console you can designate specific ports to always or never forward multicast packets.

Forward with High Priority

When “Forward with High Priority” is checked, any IGMP packets received by the switch will be forwarded in a prioritized manner, preceding packets with normal priority.

The Spanning Tree Protocol

The Spanning Tree Protocol (IEEE 802.1d) maintains a loop-free topology in networks with redundant bridges or switches. The spanning tree devices determine which devices will be active and which will be backups so that no two nodes in a network have more than one active path between them at any time. The Spanning Tree Protocol uses the most efficient path between segments. If a bridge or switch fails, the other bridges and switches reconfigure the network automatically. When the problem is repaired, the bridges and switches automatically return to the original network configuration.

Figure 7-6. Switch Device Features

If you have configured VLANs for the switch (you must do this with the device console), select a VLAN for which the features will apply.

Configuration - Support/Mgmt URLs

Support URL

To go directly to the HP Support Site on the World Wide Web, click on the **Support** tab. You will launch the site indicated by the URL that has been entered in the Configure - Support/Mgmt URLs page. By default this is the HP Network City support site. The Network City site has information about HP devices, FAQs, firmware upgrades, white papers on current technologies, and much more. This URL is:

http://www. hp.com/go/procurve

If you want to change the URL that is accessed when the Support tab is selected, type in the new address and click on the **Apply Changes** button. For example, you could change the URL to launch your site home page.

Figure 7-7. Setting URLs for Support and the Management Station

Management Server URL

Enter the URL for your management server. This will let you display the online help at any client in the network.

Note: This field will contain the address for the HP Network City web site by default. If you do not change it, the online help will be loaded from the HP Network City site.

8

Setting Up Security for a Device

It is advisable to set up security for your devices to prevent unauthorized access to the device or the network. You can configure device security to prevent unauthorized use of certain parts of the network by certain nodes, and to keep unwanted traffic out of certain parts of the network.

Note: For older HP devices that cannot be managed with a Web browser, read the chapter "Management for Non-Browserable Devices" or see the online help.

This chapter contains information on:

Device Passwords

Assigning passwords to devices helps limit access to authorized persons. In the Security page, select the **Device Passwords** button to assign passwords for the device.

Figure 8-1. Assign Passwords to a Device

There are two categories of passwords:

- Operator (Read only): The Operator can view all pages except the Security pages. For switches, this password is the same as the console password.
- Manager (Full Read and Write permissions): The Manager can view all pages and make any changes in any page. The Manager name and password are the same as the name and password used in accessing the device through the console or a telnet session. If you change the password in this page, the console password is overwritten and becomes this password.

Enter the desired names and passwords. The minimum recommended setup is to have one Manager password. Click on the **Apply Changes** button. If you want to clear these changes select the **Clear Changes** button. This will not clear any changes that you have already applied to the device.

Manager/Operator Password Combinations

The level of protection and the access granted to the device depends on what passwords are set at what levels. The table below describes the settings and their consequences.

Table 8-1. Manager/Operator Password Combinations

Passwords	Read Protected	Write Protected	Results
Manager password set Operator password not set	N/A	Yes	Anyone can get Read Access, but only the Manager can read and write to the device. Recommended minimum setting.
Manager password set Operator password set	Yes	Yes	Both the Manager and the Operator have Read Access, but only the Manager has Write Access. Everyone else is shut out of the device. Recommended setting.
Manager password not set Operator password set	Yes	Yes	The Operator has both Read and Write Access because Write Access has not been reserved for the Manager.
Manager password not set Operator password not set	N/A	N/A	Anyone can get Read and Write Access to the device. Not recommended.

See the online help for information about non-browserable devices.

The Function of Community Names

A community defines authentication and access control between an SNMP agent and a management station. The community name functions as a password in that management stations must use the community name for all Get and Set operations. This is different and separate from the Operator and Manager passwords, which protect access to the browser interface and console settings.

To set a Community Name for a device:

1. Right mouse click on a device symbol and select **SNMP Configure HP Hub/Switch**
2. Enter the passwords in the Set SNMP Passwords (Communities) page.

Port Security

You can assign security levels on hubs port by port. Select the **Port Security** button to view the current settings for each port.

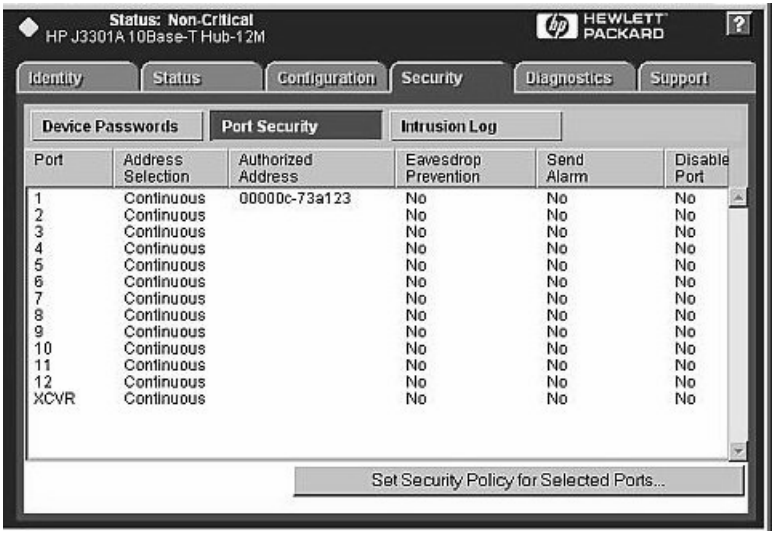

Figure 8-2. View the Security Settings for Each Port.

Address Selection

Address Selection refers to how the authorized address for a port is discovered. The three settings are explained in the table.

Table 8-2. Address Selection

Setting	Description
Continuous	The device learns the address of the device attached to the port and makes it the authorized MAC address. If a different device is later attached to the port, the new address is learned and becomes the authorized address.

Table 8-2. Address Selection

Setting	Description
First Heard	The device learns the address of the device attached to the port and makes it the authorized MAC address. If a different device is later attached to the port, the new address is registered as an "intruder address"; a security violation has occurred and the port is automatically disabled.
Assigned	Enter the address of the device that is authorized to be attached to the port. If a different device is attached to the port, the new address is registered as an "intruder address"; a security violation has occurred and the port is disabled.

To set the Address Selection:

1. Click on the **Set Security Policy for Selected Ports** button.
2. Select a setting from the **Address Selection** drop down list.
3. Click on **Apply Settings**.

Authorized Address

The Authorized Address field contains the MAC address of the device that is authorized to be attached to the port.

Eavesdrop Prevention

Eavesdrop Prevention is a feature of several HP devices that stops a computer or other device from seeing network traffic that is not intended for that port. When Eavesdrop Prevention is configured on a port, the port's authorized MAC address is compared with the destination address of any outbound packets.

Set the Eavesdrop Prevention parameter for a port or group of ports by clicking on the **Set Security Policy for Selected Ports** button and selecting "yes" from the Prevent Eavesdropping drop down list.

Send Alarm

If you set the Send Alarm parameter to "yes", a trap will be sent to the management station when an unrecognized address is received. Set the Send Alarm parameter for a port or group of ports by clicking on the **Set Security Policy for Selected Ports** button and selecting "yes" from the Send Alarm drop down list.

Note: In order for traps to function, you must also set the trap in the Thresholds dialog box, as follows:

1. Using the right mouse button, click on the device symbol in the HP Network Node Manager map.
2. Select **SNMP Configuration**.
3. Select the Thresholds tab and set the thresholds for the traps you are interested in receiving.
4. Select the Trap Receivers tab and set the management stations that can capture traps.
5. Select the Authorized Managers tab and set the management stations that can send and receive SNMP requests for the device.

Disable Port

If the Disable Port parameter displays “yes”, the port may be disabled when an unrecognized address is received. Disabling the port depends on the Address Selection parameter that you have chosen. The settings **First Heard** and **Assigned** will disable the port if a new address is heard on that port. The port will not be disabled when a new address is learned if the setting is **Continuous**.

Set Security Policy for Selected Ports

You can set the security policy port by port, or by selecting a group of ports. Select one port by clicking on the entry in the Port Security page. To select more than one port, you can Ctrl-click on each port you want to include, or to select a range of contiguous ports, click on the first port in the range, then shift-click on the last port to be included. Click the **Set Security Policy for Selected Ports** button. Select the parameters that you want to assign.

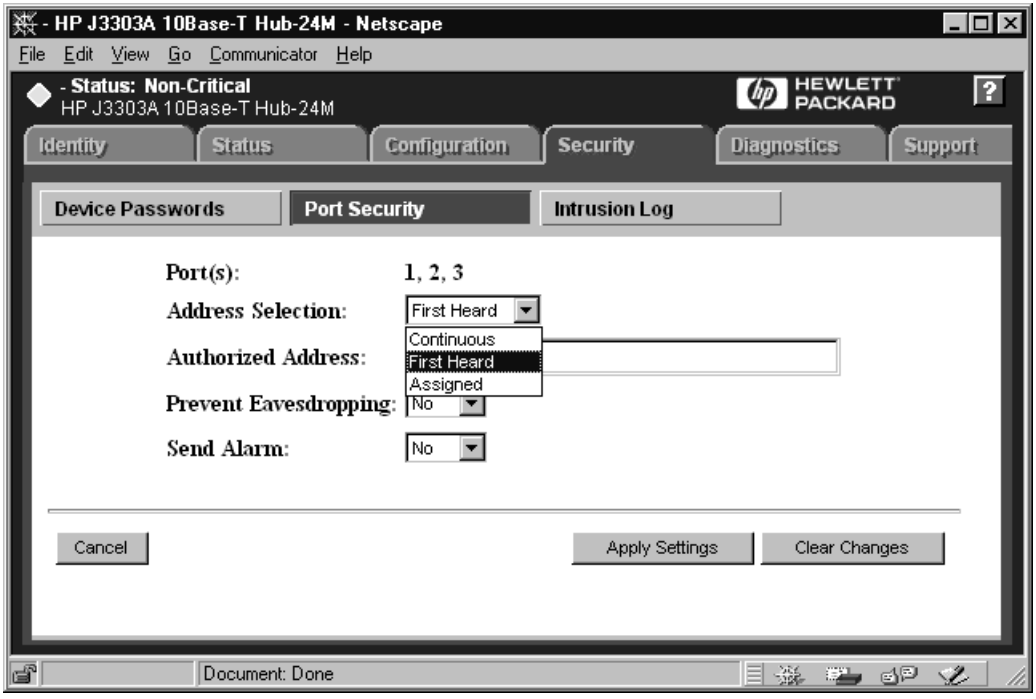

Figure 8-3. Setting Security Policy for Several Ports

The Intrusion Log

The Intrusion Log page lets you view security intrusions (violations) of a device. The information displayed includes:

- Port - The ports that have detected attempts of unauthorized access.
- Intruder Address - Address of the intruder. The IP address is displayed for SNMP agent violations. The MAC address is displayed for port violations. The port violation must be cleared before another port violation will display.
- Date/Time - Date and time the security intrusion occurred.

Performing Diagnostics

Using HP Hub & Switch Management, you can help isolate faults by running device self-tests, Link tests, and Ping tests (IP networks).

Note: For older HP devices that cannot be managed with a Web browser, read the chapter "Management for Non-Browserable Devices" or see the online help.

This chapter includes information on:

Performing a Ping/Link Test

You can isolate faults by running Link tests or Ping tests (IP networks). Select the **Diagnostics** tab and click on the **Ping/Link Test** button. Choose a test for sending test packets to, or through, a device in order to verify the path between two network devices. In the **Destination MAC/IP Address** field enter the IP address or MAC address of the device for which you want to test the connection. Specify the number of packets to send and the timeout (in seconds) for each test. Click on the **Start** button to start the test. Click on the **Stop** button to stop the test.

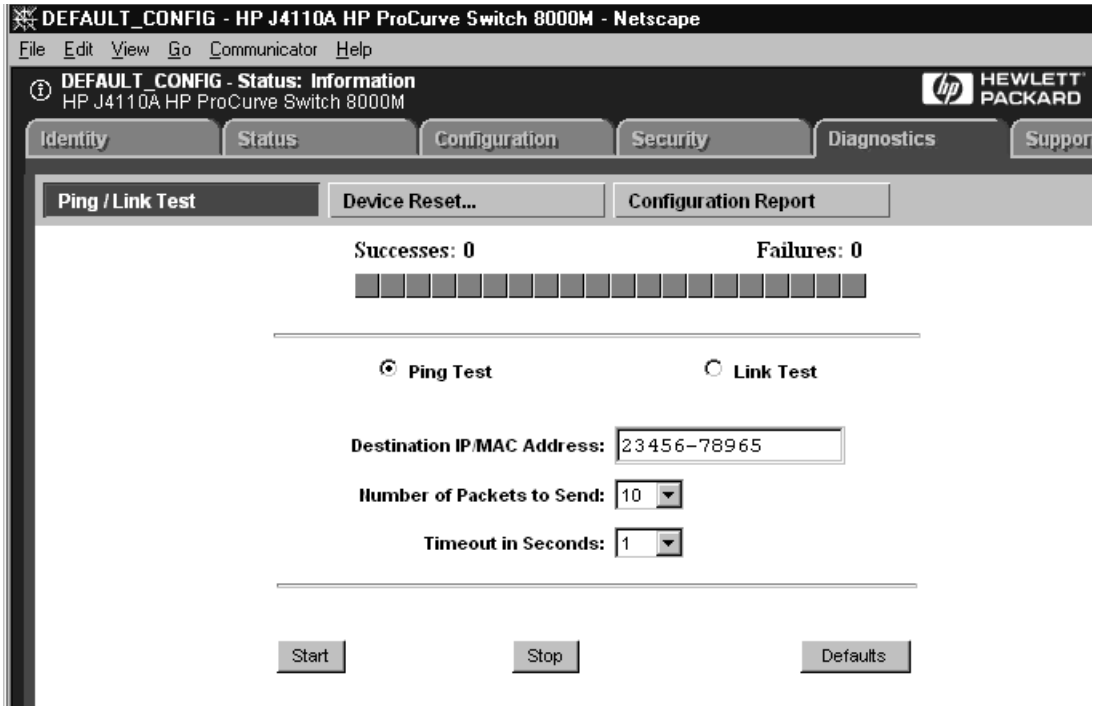

Figure 9-1. Ping/Link Test

The number of successes or failures of the test packets reaching the Destination IP or MAC Address are displayed at the top of the page. A failure means that either the device at the destination address did not respond within the timeout specified, or the data returned from the device indicated an error.

The Defaults button will reset the **Number of Packets to Send** and the **Timeout** value to the default values of 10 packets and 1 second, respectively.

Rebooting a Device

Rebooting the device is the same as powering off the device. Network operation will be interrupted while the device initializes.

Resetting a Hub to Factory Default Settings

Resetting the hub to the factory default settings removes any configuration changes that you have made since installing the device, and restores the factory defaults. The IP address is also removed; you must enter an IP address before the device will operate on your network, unless you have Bootp or DHCP.

Producing a Configuration Report

The Configuration Report displays information about the current settings on your device. You can use your browser's capabilities to print a copy of the report or save it to a file. See the online help for a more detailed explanation of this report.

HP Hub & Switch Management Admin

HP Hub & Switch Management Admin is an administration utility that allows you to set specified configuration and control parameters used by HP Hub & Switch Management for OV-UX. HP Admin is automatically installed when you install HP Hub & Switch Management for OV-UX.

This chapter includes the following topics:

Starting HP Hub & Switch Management Admin

You can start HP Admin in the following ways:

- Enter `/opt/HPASA/bin/admin` at the command line prompt.
- In an OpenView submap, display the **Options** menu and select **HP Hub & Switch Admin**.

HP Admin Parameters

The parameters that you can set in HP Admin are grouped into these categories:

- Network parameters
- User Interface parameters
- Graph options parameters
- Printer Configuration parameters
- OpenView Configuration options

The parameters are briefly described below. For more information, see the HP Admin online help.

Network Parameters

Network parameters enable you to set values and behavior for network device communication and Closeup View activity. The parameters for network device communication are described in the following table.

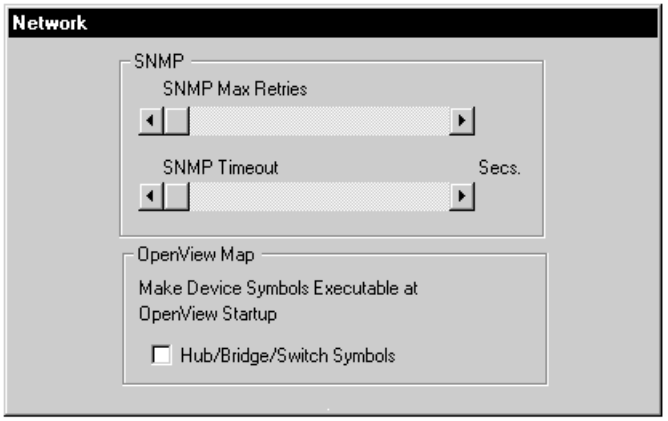

Figure 10-1. Setting Network Parameters

Table 10-1. Network Parameters

Parameter	Description
SNMP Max Retries	Specifies the number of times will retry an SNMP request to get a response. The range is 1-5 times. The default is 3.
SNMP Timeout	Specifies the time (in seconds) that HP Hub & Switch Management will wait for a reply on each request. The range is 1-6 seconds. The default is 5.

HP OpenView Device Symbols

There are two states for an OpenView device symbol on an OpenView map, ***explodable*** and ***executable***. When the device symbol is in the explodable state (no box appears around it) and you double-click on it, a submap showing

the attached devices appears. When the device symbol is in the executable state (a box appears around the symbol) and you double-click on it, a Closeup View of the device appears.

HP Admin gives you two check boxes in the **Make Device Symbols Executable at OpenView Startup** section that allow you to change the state of the device symbols the next time OpenView is started. If the check box for Hubs/Bridges/Switches is enabled (box is darker), the next time that OpenView is started the associated device symbols will be executable. If the check box is not enabled, the next time that OpenView is started the state of the symbols will not have changed. If the symbols were in the executable state when you exited OpenView, they will remain in the executable state. If the symbols were in the explodable state when you exited OpenView, they will remain in the explodable state.

Note: When an HP Admin check box is disabled, no change in the existing device symbol state occurs when OpenView is restarted.

Note: If you enable a Hub/Bridge/Switch check box while OpenView is running, the change in symbol state to executable will not occur until OpenView is restarted. OpenView checks these parameters at startup.

User Interface Parameters

User Interface parameters enable you to set the visual environment and object attributes in the HP Hub & Switch Management Device Views.

Table 10-2. User Interface Parameters

Parameter	Description
User Level	• This parameter controls HP Hub & Switch Management messages to the user. There are 3 user-level parameters: • Beginner (User Level 1, default): Message boxes will notify the user when device parameter modifications have completed. Also, the user will be warned about changes that are about to be made to a device or to a local file. The user will be allowed to cancel the change. • Intermediate (User Level 2): The user will be warned about changes that are about to be made to a device or to a local file. The user will be allowed to cancel the change. • Advanced (User Level 3): There will be no notification or confirmation messages.
Port Statistics Interval	This parameter is set by a sliding bar and specifies the sampling interval (in seconds) for the port statistics graphical displays. The default is 5 seconds.
Show Tool Bar Banner	This parameter specifies whether the title of each Toolbar button is displayed in the graphical control panels (Closeup Views) as the mouse cursor is passed over the button. The default is for button titles to be displayed.
Closeup Status Interval	This parameter is set by a sliding bar and specifies the sampling interval (in seconds) for port status in the graphical control panels (Closeup Views). The default is 10 seconds.
Closeup Gauge Interval	This parameter is set by a sliding bar and specifies the sampling interval (in seconds) for the “LAN Activity%” and the “Collision%” gauges in the graphical control panels (Closeup Views). The default is 5 seconds.
Thresholds: Activity%	Sliding bars are used to specify the levels at which the “LAN Activity%” gauges in graphical control panels (Closeup Views) change color from green to yellow, and from yellow to red. The default levels are 30% and 50%, respectively.
Thresholds: Collision%; High Priority	Sliding Bars are used to specify the levels at which the “Collision%” gauges in graphical control panels (Closeup Views) change color from green to yellow, and from yellow to red. The default levels are 30% and 50%, respectively.

Graph Options Parameters

HP Admin graph options parameters enable you to control different aspects of the graphing feature. The parameters are described in the following table.

Table 10-3. Graph Option Parameters

Parameter	Description
Graph Log Format	This parameter allows you to choose the format of the information logged to a graph log file from the Graph Counters function. • Text: Data will be logged to the log file as straight ASCII text. The default is "Text". • Spreadsheet-Tab: Data will be logged to the log file as ASCII text separated by tabs for ease of exporting the data to spreadsheets that use tabs. • Spreadsheet-Comma: Data will be logged to the file as ASCII text separated by commas for ease of exporting the data to spreadsheets that use commas.
Graph Digits to Display	This parameter is set by a sliding bar and specifies the maximum number of digits displayed for a counter value before displaying the value in scientific notation. The default is 4.
Graph Interval	This parameter is set by a sliding bar and specifies the default sampling time interval (hh:mm:ss) for graphing. The minimum setting is 1 second. The maximum value is 9999:59:59. The default is 20 seconds.
Graph Log File	The parameters set in this section specifies the file name for the graph log file and the size of the log file. Default log file name is "graphs.log" Default log file size is 128000 bytes. The minimum log file size is 10000 bytes. The maximum is 2^{32} -1 bytes.
Enable Graph Sensitive Scaling	This parameter controls the scaling of graphs. The default is "disabled". If enabled, the "Y-axis" graphing scale will automatically adjust to display only the range of values needed. A more detailed view of the graph will be displayed. If disabled, the "Y-axis" graphing scale will start at zero. The upper limit will automatically adjust to the power of 10 as needed.

Printer Configuration Parameters

Network management applications that implement printer support on X Window systems can use the Print Configuration dialog box to configure printer configuration parameters.

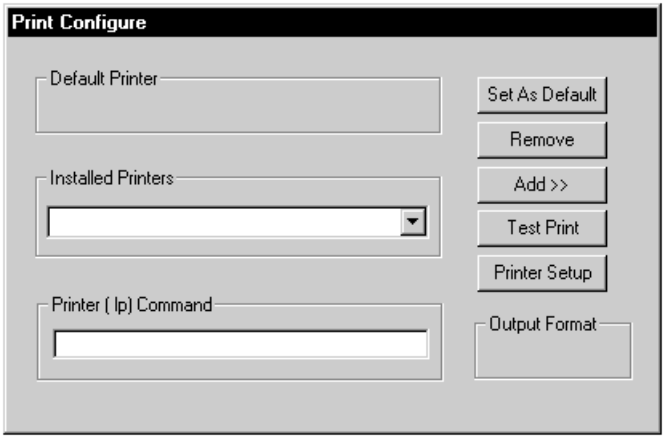

Figure 10-2. Printer Configuration

Table 10-4. Printer Configuration Parameters

Parameter	Description
Default Printer	Displays the current default printer name. This printer will be used if the choice of printers is not overridden.
Installed Printers	Provides a sorted list of all currently configured printers. The currently displayed printer updates the “lp command” and “Output Format” boxes.
lp command	Shows the device name and port for the currently selected printer, and the lp command string. The lp command is used to redirect the output to a specific device—printed output is “piped” into the command specified by the lp command text. Your can modify the lp command string to meet your printer requirements. See your HP-UX man pages for more information on the lp command.
Output Format	Identifies the driver type of the printer that is currently selected. The lp command string must be compatible with the format identified in this box. You may need to edit the lp command string or choose another printer.

Table 10-4. Printer Configuration Parameters

Parameter	Description
Set As Default	Sets the printer selected in the "Installed Printers" box as the default printer.
Remove	Removes a selected printer from the "Installed Printers" list.
Add	Displays a list of supported printers that you can select and add to the "Installed Printers" list.
Test Print	Prints a sample test file to a selected printer if the printer configuration has been saved (see the OK button).
OK	Saves the configuration and returns to the main HP Admin dialog box.
Cancel	Returns to the main HP Admin dialog box without saving configuration changes.
Help	Accesses the HP Admin online help system.

OpenView Configuration Options

You can change the way that OpenView and HP Hub & Switch Management interact by setting these options:

- ForceMapUpdates
- NoMapWalk
- Trace
- Distributed Console

These options provide advanced tuning capabilities for knowledgeable users of OpenView. You do not need to use them to run the application.

Any changes that you make will not take effect until the next time that OpenView (ovw) is run.

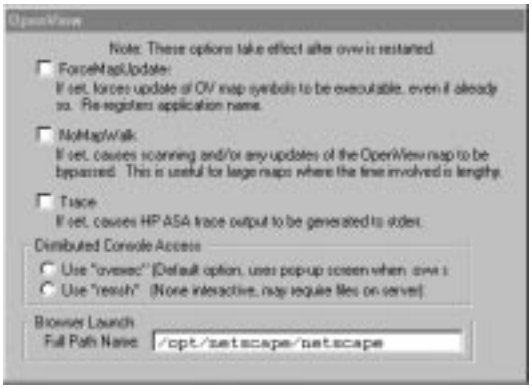

Figure 10-3. OpenView Configuration Options

The options are described in more detail here.

ForceMapUpdates. If the attributes (name of icon, application name) of a symbol are changed, for example, during an update, the symbol must be re-registered with OpenView for the changes to take effect. Selecting this option will update the symbol the next time that the master copy of OpenView (ovw) is run. If this option is not set, symbols that are already executable are not updated with the new information.

NoMapWalk. When you start HP Hub & Switch Management, it can take a long time to scan ("walk") a large OpenView map to get the information needed to provide full functionality. When the NoMapWalk option is selected, HP Hub & Switch Management start up time is greatly decreased.

When NoMapWalk is enabled, the symbols of newly discovered devices will not be executable with a double-mouse-click. You must click on the device in the OpenView map, then use the Monitor menu (select HP Hub/Bridge) to display the device's Closeup View. You also will lose the ability to perform batch security settings.

Trace. This option is provided to assist support personnel in tracking down problems related to OpenView integration with HP Hub & Switch Management. Do not set this option unless you are told to do so by support personnel.

Distributed Console. HP Hub & Switch Management is started remotely when you use Network Node Manager's Distributed Console feature from a client station. The program "ovexec" displays a pop-up window in which you enter a password for the remote system. If you do not want this pop-up to be displayed, that is, you do not wish to enter a password, select the "remsh" option to start HP Hub & Switch Management remotely.

Note: If you select "`remsh`", the name of your client machine must be in the `/etc/hosts.equiv` file or the `$HOME/.rhosts` file on the remote system. Refer to these man pages for more information on these files:

man `hosts.equiv`

man `rhosts`

Browser Launch. You can enter the full path name for the browser that will launch when you click on a device that is manageable with a browser, for example:

```
/opt/netscape/netscape
```

Management for Non-Browserable Devices

This chapter provides a summary of hub, bridge, and switch management functions for devices that cannot be managed with the Web browser interface. It includes the following topics:

Use the online help for more information about specific device functions.

About Closeup Views

HP Hub & Switch Management provides direct access to HP hub, bridge, and switch management for devices that are not manageable with a Web browser through graphical control panels, or Closeup Views. If you have switching hubs, you can also use the Closeup View to create and modify segments in your network.

A Closeup View is an interactive, visual display of a device. You can use the Closeup View to obtain device status, and run Hub & Switch Management command functions through push-button icons and menus. There is a Closeup View for most HP managed devices.

There will be differences in the available function icons depending on the device type. Icons for functions that are not available for some devices will either not be selectable (grayed out) or will not appear. Also, menu options launched from icons that are not available for some devices either will not appear, or if they appear, they will not be selectable. For information on device management functions for any particular device, refer to the online help in the Closeup View.

For HP AdvanceStack hubs, Closeup Views are available for managing all hubs on a Distributed Management Chain. Closeup Views for chained hubs that are without SNMP modules are accessed through the appropriate SNMP-based hub's Closeup View. Functions that are not available for chained hubs will not be selectable.

Note

HP Hub & Switch Management now supports non-pulick community names when displaying the Closup View. For configuring non-public community names, refer to the HP OpenView *Using Network Node Manager* manual.

Displaying the Closeup View

You can display a Closeup View in several ways, including the following:

- From an HP OpenView map, use the left mouse button and ***double-click*** on a hub, bridge, or switch symbol.
- On an HP OpenView map, select a hub, bridge, or switch symbol. Then display the Monitor menu and select **HP Hub/Switch**.
- From a Closeup View of an SNMP-based AdvanceStack hub, display the list of chained hubs by clicking on the Chained Devices button. The list displayed identifies each chained hub by MAC address and hub type. Select the MAC address for the desired hub.
- Right-mouse-click on a device symbol and select **Monitor HP Hub/ Switch.**

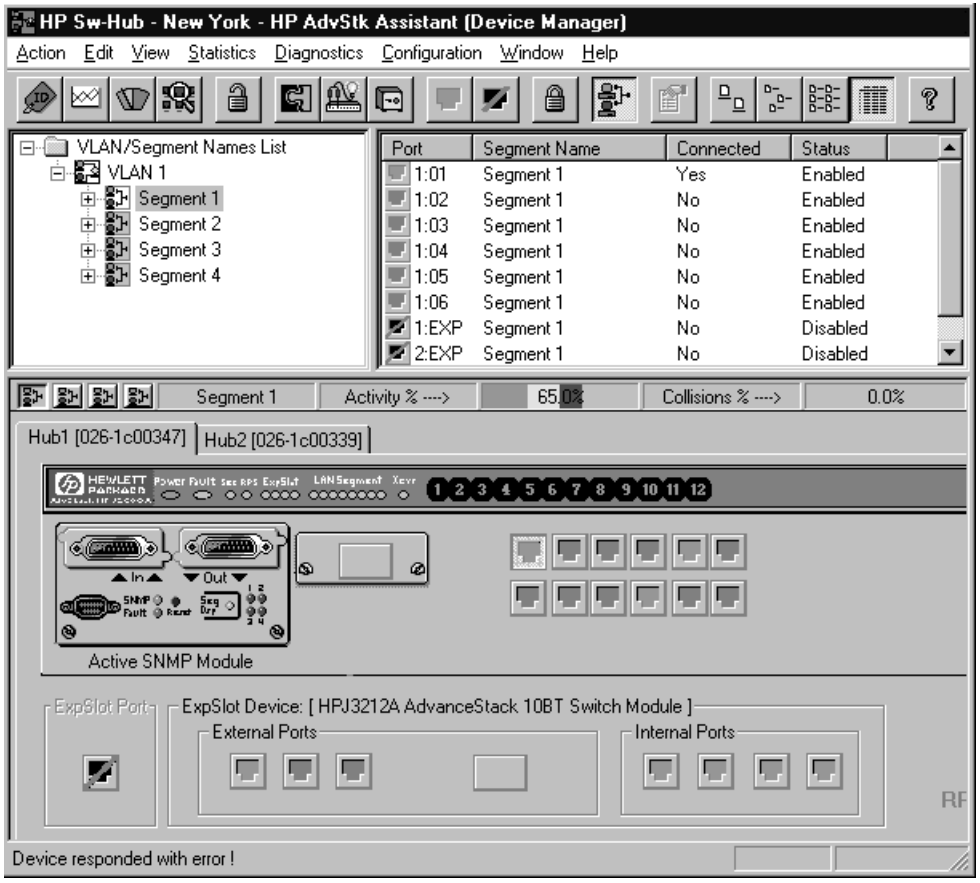

Figure 11-1. Switching Hub Closeup View

The number of Closeup Views that you can display at one time depends on your free system resources available (such as available memory).

If the HP device can be managed with your browser, the menu option **SNMP Configure HP Hub/Switch** will also display when you right-mouse-click on a device symbol. Selecting this feature allows you to configure community names and authorized managers for the device. See the online help for configuration instructions.

Closeup View Areas

The regions of the Closeup View are discussed below.

Title Bar

At the top of the Closeup View is a title bar that displays the device type and its network address.

Message Bar

The Message Bar is along the bottom of the Closeup View. It is primarily used to identify, or describe the purpose of, various items in the view. Simply place the cursor on an item and read the appropriate box in the Message Bar.

If a port is selected, the center box in the Message Bar identifies the selected port (for example, “Port A9”).

Toolbar

The Toolbar contains buttons to perform Hub & Switch Management commands and functions. If you place the cursor over a Toolbar button, message bar text is displayed that identifies the command or function. (See the online help for a description of the Toolbar icons.)

Activity Gauges

Two linear bar charts, or “gauges”, are displayed on most Closeup Views. These gauges provide indications of LAN traffic sampled by the device. The gauges are:

- Activity%—Represents the total LAN activity viewed by all segments attached to the device as a percent of the total bandwidth of the segments.
- Collisions%—Shows the total collisions viewed by all segments attached to the device as a percentage of total packets seen by these segments.

Hub LAN Ports

The Closeup View allows you to view each hub port and determine port status. Port status can be determined by the port icon symbol and colors displayed.

You can individually select any port on a Closeup View by clicking on the port itself. The port number will be displayed in the message bar. If you select a port, you can perform management functions through the applicable Toolbar button. (If passwords are used, you must be logged onto the hub to change a port's configuration.)

Overview of Toolbar Functions

HP Hub & Switch Management device functions in the Closeup Views allow you to configure, monitor and manage HP hubs, bridges, and switches.

The following table summarizes the Toolbar menu functions in the Closeup Views. For specific information about how to use a particular device function or menu dialog box, click on the **Help** button in the dialog box.

Table 11-1. Summary of Toolbar Functions

Icon	Toolbar Button	Description
	Device ID	Displays identification information for an HP hub, bridge or switch. For example, you can determine the device type, firmware version, and MAC address.
	Graph Counters	Displays the Graph Counters - Graph window for graphing various counters and statistical formulas on a device. The default graph is the LAN Activity% statistics. If you position the cursor over the graphing area and press the right mouse button, a pop-up menu is displayed. Select “Options” to modify the counters and devices for graphing, and to configure other graphing options.
	Port Statistics	Displays gauges for viewing statistical counters for a segment and selected ports on the segment. • Hubs: gauges for LAN Activity, Error Packets, and Broadcast Packets are displayed. • Bridges: gauges for Broadcast Packets, Packets Forwarded, Packets Filtered, and Error Packets are displayed. • Switches: gauges for LAN Activity, Packets Forwarded, Packets Filtered, Broadcasts Received, Collisions, and Errors Received are displayed.
	Port Statistics Summary	Displays an information window that lists important statistics and counter values for each port on the device. The displayed counters will differ depending on the device type (for example, 10Base-T hub, 100VG hub, 10/100 switch, or bridge).

Table 11-1. Summary of Toolbar Functions

Icon	Toolbar Button	Description
	Logon	Displays a Logon dialog box. If a hub, bridge or switch has a password, you must first log on to it before you can change configuration or security features, or run diagnostic tests. Logon passwords are set up using the Configuration button (select Set Administration). If you forget a password, you may need to go to the device to clear the password (see your device manuals).
	Configuration	Displays a tabbed dialog box for device configuration (The tabs displayed depend on the device): • Administration • IP Config • Thresholds • Port Configuration • Backup Links • Upload • Download • Monitor Port • Address Table • Wild Character Filter • Spanning Tree • Bridge Configuration
	Diagnose	Displays a pop-up menu list of device or network test functions. The tests that can be performed depend on the type of device.
	Security	Displays a tabbed dialog box for configuring security: • Authorized Managers: The network management stations that can send and receive SNMP requests for this device. • Community Names: Names that are valid for SNMP requests to the device or stack of hubs. A read and write level are specified for each community name. • Security Policy: Set global security for all devices of the same type on your network. • Port Security: Configure Intruder Detection and Eavesdrop Prevention for each port. • Intrusion Log: View security intrusions for a device.

Table 11-1. Summary of Toolbar Functions

Icon	Toolbar Button	Description
	Enable Port	Enables a selected hub port. If a password is assigned to the hub, you must log on to the hub before you can change the state of a port.
	Disable Port	Disables a selected hub port. If a password is assigned to the hub, you must log on to the hub before you can change the state of a port.
	Logoff	Displays a Logoff dialog box. If a hub or bridge has a password, you can log off the device to prevent configuration changes.
	VLAN Configuration	Displays the VLAN Configuration window.
	Properties	Displays a dialog box that allows you to view or change information about a selected VLAN or segment: • Port number • Name of VLAN • Connected status • Enabled/Disabled status • Active status • Protocol type
	Large icons	Displays ports as large icons.
	Small icons	Displays ports as small icons.

Table 11-1. Summary of Toolbar Functions

Icon	Toolbar Button	Description
	List	Lists all port icons in rows.
	Details	List information with each port: • Port number • Segment to which the port belongs • Connected status: indicates whether the port is currently connected to a device • Status: the port is enabled or disabled.
	Help	Runs the Hub & Switch Management online help system.

Configuration Functions

The Configuration button displays a menu that allows you to perform configuration functions for the device. The menu items displayed depend on the type of device.

See the online help for details about the Configuration menu items.

Setting the Configuration Parameters

When you select the Configuration icon, the Configuration tabbed dialog box displays. By clicking on the appropriate tab, you can configure parameters for your devices as well as performing software uploads to and downloads from a configuration file. See the online help to obtain instructions for configuring a specific function.

A

Appendix A

Appendix A contains the following topics:

Agent Firmware Versions

HP Hub & Switch Management communicates with network devices using SNMP (Simple Network Management Protocol).To access device features, each network device must contain a compatible version of agent software or firmware.

Note: The latest firmware agents can be obtained from the Support section of the HP networking Web page. The URL is:

http://www.hp.com/go/procurve

Verifying Device Agent Versions

You can check the agent version on an HP device using one of the following methods:

- Use the device's console port interface (a ***non-network*** connection).

  You can connect a terminal or computer directly to the device or through a modem. Refer to the device's *Installation and Reference Guide* for use of the device's RS-232 console port.

  - For HP devices, you can use an ASCII terminal or computer with VT 100 terminal emulation.
- Use an available network application (a ***network*** connection).

For HP devices, use an existing version of HP Hub & Switch Management or other device management utility.

Update the device's software or firmware to the current supported version.

Note: HP Hub & Switch Management may be able to discover devices that have previous versions of device agent firmware. However, the use of some functions may be limited.

Preparing Network Devices

For HP Hub & Switch Management to communicate with devices on your network, the network devices must:

- have SNMP agent firmware that is compatible with this version of HP Hub & Switch Management.
- for IP networks, have a unique IP network address.

Note: Hubs and bridges shipped prior to July 1992 must be upgraded.

Basic hub management features are available for chained AdvanceStack hubs if they are connected to an SNMP-based hub of the same media type (10Base-T or 100VG) over a Distributed Management chain.

Device Network Addresses

On an IP network, each managed device must have an IP address. If you intend to run HP Hub & Switch Management on an IP network, you must configure the IP address for each device you want to manage.

IP addresses are normally configured when the device is installed. For HP hubs, bridges, and switches, IP addresses are configured using the console port interface. For more details on console port connection and available commands, see the device's *Installation and Reference Guide*.

Note: You can use HP Hub & Switch Management to change an IP address on a hub after it has been assigned, but not on a switch or a

bridge.

Globally Assigned IP Network Addresses

If you intend to connect your network to other networks that use globally administered IP addresses, Hewlett-Packard strongly recommends that you use IP addresses that have been assigned to you. There is a formal process for assigning unique IP addresses to networks worldwide. Contact one of the following companies:

United States and countries not in Europe or Asia/Pacific	Network Solutions, Inc. Attn: InterNIC Registration Service 505 Huntmar Park Drive Herndon, VA 22070	1-703-742-4777 questions@internic.net http://rs.internic.net
Europe	RIPE NCC Kruislaan 409NL-1098 SJ Amsterdam The Netherlands	+31 20 592 5065 ncc@ripe.net http://www.ripe.net
Asia/Pacific	Attention: IN-ADDR.ARPA Registration Asia Pacific Network Information Center c/o Internet Initiative Japan, Inc. Sanbancho Annex Bldg. 1-4 Sanban-cho, Chiyoda-ku Tokyo 102, Japan	domreg@apnic.net http://www.apnic.net

For more information, refer to ***Internetworking with TCP/IP: Principles, Protocols and Architecture*** by Douglas E. Comer (Prentice-Hall, Inc., publisher).

Configuring IP Parameters

To run HP Hub and Switch Management on an IP network, you must configure the management station and all managed devices for IP.

The network management station is configured for IP using the TCP/IP stack utilities. To configure a device for IP, you typically connect to the device's console port and use the console port interface. (Refer to the device's installation manual for more information.)

Before you configure the network management station and manageable devices for IP, make a list of all the devices on the network and what their IP addresses will be.

Note: Make sure that every device has a unique IP address. Make sure that all devices on a given IP network number have the same subnet mask.

The IP configuration parameters are described below.

IP Address . The IP address of the hub, bridge, or switch is written in the format X.X.X.X, where each X is a decimal number between 1 and 254. Every IP address on a network must be unique.

The default value, 0.0.0.0, disables IP communications. Use the default value only if you are not going to manage the device with HP Hub & Switch Management and you want to disable IP communications for that device.

Subnet Mask. The bit mask defines which portion of the IP address is the subnet address and is written in the format X.X.X.X. The default value is automatically generated and depends on the class of IP address that you entered. See your network administrator for the subnet mask address. All devices on a given IP network number must use the same subnet mask address.

Primary Default Router . The routing IP address of the nearest router in your network. The default is 0.0.0.0.

Backup Default Router. The IP address of the router to use when the primary default router is inaccessible. The default value is 0.0.0.0. If there is no backup router and no primary default router, use the default.

Time To Live . The number of IP routers a packet is allowed to cross before the packet is discarded. The default value is 32. Increase this value if the hub, bridge, or switch is managed from a network management station that is more than 32 routers away. The maximum allowable value is 255.

Note: For selected devices, such as the HP J2980A AdvanceStack 10/100 LAN Switch-16, you must preconfigure the SNMP community

name “public” on the device to allow the device to be discovered and managed by HP Hub and Switch Management. Typically, the community name on HP hubs and bridges will automatically default to “public”.

To configure a device for IP networks, use the device's console port interface. Refer to the device's Installation and Reference Guide for use of the device's RS-232 console port.

Note: For HP hubs, HP Hub & Switch Management can be used to *change* IP addresses after they have been initially assigned during installation.

Network Bootp Server

HP EtherTwist Hub Plus/24S and HP AdvanceStack 10Base-T hubs (with SNMP modules installed) support the use of Bootp (Bootstrap Protocol) to automatically retrieve their IP configuration from a server on the network. A device's IP configuration must be configured in a file on the Bootp server. When the device is powered on, Bootp is used to automatically download the IP configuration to the device.

- Each device that supports Bootp must have Bootp enabled to retrieve its IP configuration from the server. The factory default setting is for Bootp operation to be enabled. You can enable or disable Bootp operation through the device's console port, or from a network management application (such as HP Hub & Switch Management).
- For more information on IP configuration using Bootp, refer to your device's *Installation and Reference Guide*.

Index

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

X